U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspections Division

Review of the United States Marshals Service Judicial Security Process

Report Number I-2004-004

March 2004

EXECUTIVE DIGEST

Protecting the federal judiciary is one of the eight strategic goals of the Department of Justice (Department),[1] and it is the primary mission of the United States Marshals Service (USMS).[2] No federal judges have been assassinated since 1989, but two federal judges have been assaulted in the last three years, and the USMS receives almost 700 threats against members of the judiciary each year. Further, in the 10 years since the first World Trade Center bombing trials, the federal judiciary has conducted an increasing number of high-threat trials, such as those involving international and domestic terrorism, international drug trafficking, organized crime, and gang activity.[3] Since fiscal year (FY) 2001, Congress has increased funding for judicial security by about 50 percent and authorized the USMS to hire 106 new Court Security Inspectors. However, Congress has expressed concern that "as the program has grown sufficient attention has not been provided to program and budget administration...."[4]

The Office of the Inspector General (OIG) evaluated the USMS's efforts since September 11, 2001, to improve its protection of the federal judiciary. We focused specifically on the USMS's ability to assess threats and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from the courthouse.

RESULTS IN BRIEF

We found that since September 11, 2001, the USMS has placed greater emphasis on judicial security by hiring 106 court security inspectors and increasing courthouse security. However, the USMS's assessments of threats against members of the federal judiciary are often untimely and of questionable validity. Further, the USMS has limited capability to collect and share intelligence on potential threats to the judiciary from USMS districts, the Federal Bureau of Investigation's (FBI's) Joint Terrorism Task

[1] U.S. Department of Justice, FY 2001-2006 Strategic Plan, November 2001, p. 99.

[2] Other major USMS missions include supporting the effective operation of the judicial system through the execution of federal warrants; housing and transporting federal prisoners in custody; and ensuring the security, health, and safety of Government witnesses and their immediate dependents.

[3] On February 26, 1993, terrorists attempted to blow up the World Trade Center by detonating a rental truck loaded with explosives in the underground parking garage.

[4] Conference Report 108-10, February 13, 2003, p. 735-736.

Forces (JTTFs), and other sources. Finally, the USMS lacks adequate standards for determining the appropriate protective measures that should be applied to protect the judiciary against identified potential risks (risk-based standards) during high-threat trials and when they are away from the courthouse.

USMS Threat Assessments are Untimely and of Questionable Validity

Timely threat assessments are essential to alert USMS districts to threats with a higher potential for violence, but the USMS routinely fails to meet its internal standard that requires threats against judges to be assessed within a specific time period.[5] We found that more than 73 percent of the threat assessments conducted from FY 2000 through FY 2003 took more than the standard time.[6] Furthermore, the USMS failed to improve the timeliness of its threat assessments despite a 30 percent decrease in the number of reported threats since FY 2000. In fact, the number of assessments that took significantly longer than the standard time to complete more than quadrupled from 24 in FY 2000 to 103 in FY 2003.

In addition to taking weeks or months to complete, the validity of USMS assessments is questionable because the historical threat database used to assess reported threats has not been updated since 1996. The database contains no information on the more than 4,900 threats made since then – including threats related to terrorism cases that have occurred since September 11, 2001.

Further, when allocating resources and determining protective measures in response to threats, the USMS continues to rely on statistics developed from the historical threat database which indicate that only about one out of every ten threats escalated or resulted in violence. Because the information in the historical threat database is outdated, we question the validity of threat assessments or resource allocations based on this data.

USMS Has Limited Capability to Collect and Share Intelligence

We also found that the USMS has limited capability to collect and share intelligence on threats to the federal judiciary among its districts and

[5] The exact time standards are considered by the USMS to be law enforcement sensitive.

[6] To obtain sufficient data for comparison we reviewed data from FY 2000 through FY 2003, two years before and two years after September 11, 2001.

its representatives on the FBI's JTTFs. The limitations persist because the USMS has neither acted on internal studies that identified the need for the USMS to improve its capability to collect and share intelligence nor updated internal guidance to implement the authority granted by Congress in the Patriot Act.[7] Specifically:

- The USMS has no central program to collect, assess, and share intelligence on threats to the judiciary. Prior to 1994, the USMS operated a centralized intelligence collection and assessment program in its Threat Analysis Division. In a 1994 reorganization, the USMS Director eliminated the Division and did not reassign its duties. After September 11, 2001, internal USMS studies identified the need for the USMS to establish a centralized program to collect and share intelligence from the districts and the USMS representatives on JTTFs. The studies also recommended that the USMS establish liaisons at the Central Intelligence Agency, the Foreign Terrorist Tracking Task Force, and the Secret Service Protective Intelligence Division, among other intelligence organizations. As of October 2003, the USMS had not developed any centralized intelligence-sharing capability.

- Outdated USMS internal guidance limits intelligence collection. An April 5, 1996, USMS Office of General Counsel (OGC) opinion, based on 1983 Attorney General Guidelines, directed the USMS to limit its collection of intelligence, including information in special databases used to track and assess threats to the judiciary.[8] The Patriot Act has since provided new authority for law enforcement agencies to collect and share intelligence related to terrorism and other threats, and the Attorney General Guidelines have been revised to reflect this new authority. However, the USMS has not revised its internal guidance to implement the new authority to collect intelligence.

- The USMS does not fully participate in the FBI's JTTFs. Some U.S. Marshals have assigned Deputy Marshals to FBI JTTFs, but

[7] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [Patriot Act], Public Law 107-56, October 25, 2001.

[8] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Domestic Security/Terrorism Investigations (March 1983) described authorities and activities related to criminal investigations. The Guidelines only mention the FBI but have been interpreted as applying to all Department criminal investigations.

the USMS has no service-wide policy to ensure that it is represented on each JTTF. As of October 2003, JTTF membership rosters provided by the FBI showed that the USMS has assigned 50 Deputy Marshals to 29 of the FBI's 56 field office JTTFs. Of the 50 Deputy Marshals, 25 are full-time representatives and 25 are part-time representatives. Further, the USMS's Memorandum of Understanding with the FBI requires that JTTF representatives have Top Secret clearances, but we found that only 33 of the 50 USMS representatives to the JTTFs had Top Secret security clearances. According to the Chairman of the USMS Executive Working Group formed by the Director in September 2001 to examine USMS intelligence capabilities, the wide spread lack of clearances is a barrier to improving intelligence collection and sharing.

- The USMS lacks the secure telecommunication systems required to effectively share intelligence on threats to the judiciary. As of August 20, 2003, only 51 of the 94 USMS districts had secure communications equipment required to transmit classified information.

In the two high-threat trials we reviewed, the USMS's limited capability to collect and share JTTF intelligence affected the USMS's efforts to protect the federal judiciary. In one trial of individuals who were providing financial aid to terrorists, the USMS did not receive classified JTTF intelligence that the district considered critical to trial security operations because the district's part-time representative to the JTTF did not have a Top Secret security clearance. In the other trial, the USMS was not informed of the imminent arrest of six terrorists identified by a JTTF investigation until just before the arrests. The short notice precluded the USMS from taking the extensive security measures required to secure a large number of suspected terrorist prisoners.

USMS Lacks Adequate Standards for Determining Appropriate Protective Measures

We found that the USMS lacks adequate risk-based standards for determining the appropriate measures to protect the judiciary during high-threat trials and to protect threatened judges away from the courthouse (protective services details). Without risk-based standards, the USMS cannot ensure that districts consistently apply similar protective measures in response to similar threats, and that limited resources for protecting the judiciary are used in the most effective manner.

High-threat trials. We found that the USMS's Policy and Procedures Manual (Manual) has not been updated in over a decade and provides limited and outdated guidance on specific protective measures for high-threat trials.[9] The Manual offers no guidance on providing security for trials of individuals associated with international terrorist groups, or for many other types of trials that present significant risks to the judiciary, such as criminal cases involving espionage, prosecutions of gang violence, and cases with cooperating witnesses. Further, the Manual does not provide guidance on the use of special equipment such as trace explosive detectors, armored cars, body armor, and enhanced prisoner restraints.

Protective services details. We found that the USMS's guidance on individual protective measures is outdated.[10] The guidance does not address the use of equipment that has become more widely available in recent years, such as perimeter cameras, car alarms, home alarms, and cellular phones, and has not been updated to account for threats that are beyond the ability of the USMS alone to mitigate, such as the threat of retaliation by international terrorists. Further, the guidance still directs readers to offices and functions that were eliminated almost ten years ago.

Although specific protective measures must be selected based on the characteristics of each individual case, in the absence of risk-based standards we found that districts did not consistently apply similar protective measures in response to similar threats. For example, one district used the USMS Special Operations Group (SOG) (a specially trained and equipped unit deployed in high-risk law enforcement situations) extensively during a high-threat trial while another did not use the SOG at all for a similar high-threat trial. Likewise, the protective services details provided judges varied significantly in the protective measures implemented. The extent and appropriateness of the protective measures applied in each case could not be evaluated fully because the USMS does not complete after-action reports on the measures taken during high-threat trials or protective services details.

[9] USMS Policy and Procedures Manual, Volume X, Judicial and Court Security, July 1, 1993.

[10] The USMS's official policy is Policy Directive 99-07, January 7, 1999, Protective Investigations. The Policy Directive does not address protective services details, but refers to guidance in *The U.S. Marshals Service Protective Investigations Program, A Procedural Handbook for Threat Investigators and Supervisors*, January 1999.

Without adequate risk-based standards, the USMS cannot effectively determine when districts should be provided additional resources to support high-threat trials or protective services details. In FY 2002, the USMS provided additional funding to districts to support 117 high-threat trials.[11] However, in response to our national survey, districts estimated that about 20 percent of all trials in 2002 involved a "substantial potential for violence." Given that there were 12,817 trials completed in U.S. District Courts in FY 2002, the number of trials with "substantial" risks could have exceeded 2,400.[12] Without adequate risk-based standards, and without after-action reports to evaluate and improve its protection of the judiciary, the USMS cannot effectively ensure that the most significant risks are addressed and that resources are used appropriately.

Conclusions

The USMS should take immediate steps to improve its ability to assess threats to the federal judiciary. Currently, USMS threat assessments are not timely and no new threat information has been entered into the historical threat database used to assess new threats since 1996. The lack of current threat information in the database undermines the validity of new assessments both for determining appropriate protective measures and for allocating resources.

While the USMS has taken steps since September 11, 2001, to evaluate its capability to collect and share intelligence, as of October 2003 the USMS had not acted on internal studies that documented the need to reestablish an intelligence program to collect, analyze, and disseminate information related to high-threat trials and threats to the federal judiciary.

Finally, the USMS needs risk-based standards for determining the appropriate protective measures that should be applied to protect the judiciary during high-threat trials and when using protective services details. In addition, current risk-based standards are also needed to more effectively identify those high-threat trials and protective services details for which the districts should receive additional resources.

[11] We asked how many requests were rejected, but the USMS Judicial Security Division (JSD) responded that it tracks only those requests that are approved.

[12] Administrative Office of the United States Courts (AOUSC) FY 2002 Annual Report, Table C-7, U.S. District Courts – Civil and Criminal Trials Completed.

Recommendations

To improve the USMS's capacity to carry out its primary mission of protecting the federal judiciary, we recommend that the USMS take the following actions:

1. Ensure that all threats to the judiciary are assessed within established timeframes.

2. Update the historical threat database or develop a new database to perform comparative assessments.

3. Assign full-time representatives to all 56 FBI field office JTTFs and ensure effective USMS liaison with intelligence agencies (e.g., the U.S. Secret Service's National Threat Assessment Center, the Central Intelligence Agency, and the National Security Agency).

4. Create a centralized capability to identify, collect, analyze, and share intelligence with USMS districts, as well as with the USMS JTTF representatives and other intelligence liaisons.

5. Require that all Chief Deputy Marshals and USMS JTTF representatives have Top Secret clearances, and ensure that each district has secure communication equipment.

6. Revise the 1993 *Judicial and Court Security Manual* and the 1999 *Offsite Security Booklet for Judicial Officers* to establish risk-based standards and require after-action reports for high-threat trials and protective details.

TABLE OF CONTENTS

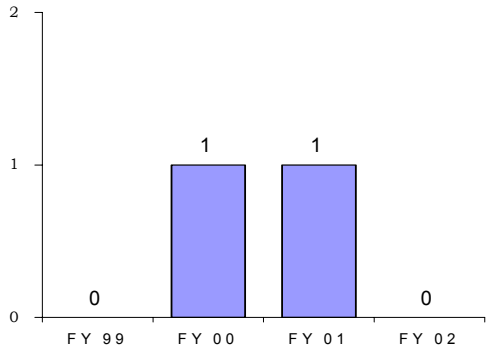
INTRODUCTION

BACKGROUND

Protecting the federal judiciary is one of the eight strategic goals of the Department of Justice (Department).[13] The United States Marshals Service (USMS) is charged with meeting that goal by protecting members of the federal judiciary, court officers, and other threatened persons.[14] To carry out its mission, the USMS Director and 94 U.S. Marshals appointed by the President and confirmed by the Senate oversee the operations of 4,761 employees (3,342 Deputy Marshals and 1,419 administrative personnel) at 350 locations around the country.

The USMS measures its effectiveness in meeting the strategic goal to protect the judiciary by tracking the number of assaults against the more than 2,000 federal judges and magistrates that the USMS protects. The target for success is zero assaults. As shown in Figure 1, there were no assaults in FYs 1999 and 2002, but there was one each in FY 2000 and FY 2001.

Figure 1 – Assaults Against the Judiciary



Source: Department of Justice
FY 2002 Performance Report

Since FY 2001, Congress has increased the USMS's funding for judicial security by approximately 50 percent. On April 1, 2003, the Attorney General asked Congress for more resources for judicial security. Stating that "[s]ecurity surrounding terrorist-related court proceedings requires an unprecedented level of protection for all trial participants because of the global interest and intense media attention," the Attorney General asked for "significant resources to improve courtroom security…

[13] Department of Justice FY 2002 Performance Report/FY 2003 Revised Final, FY 2004 Performance Plan, February 2003.

[14] Other USMS missions include ensuring the security, health, and safety of government witnesses and their immediate dependents; maintaining custody, housing, and transporting federal prisoners; and executing federal warrants.

associated with terrorist-related court proceedings."[15] While increasing funding for judicial security, Congress also has expressed concern that "as the program has grown sufficient attention has not been provided to program and budget administration…."[16]

The USMS Judicial Security Division

The USMS Judicial Security Division (JSD) provides for the general security of federal courthouses, federal courtrooms in other buildings, and the personal security of the federal judiciary when they are most vulnerable – away from their courtrooms and chambers.[17]

In FY 2002, the JSD supervised security for 117 high-threat trials, coordinated 150 personal protective services details for Supreme Court Justices traveling outside the Washington Metropolitan Area, and coordinated security for 165 judicial conferences and 20 other events attended by the federal judiciary. The JSD directs the following three program areas.

High-Threat Trials

Although trials with greater than normal risk may be referred to as "high risk", "high profile," "high visibility," or "sensitive" trials, the term "high-threat trial" is most commonly used by the USMS and by Congress. Recent high-threat trials included:

- In Charlotte, North Carolina, members of a cell who provided material support to Hezbollah pled guilty to conspiring to aid terrorism (June 2002).
- In Buffalo, New York, members of a "sleeper cell" (commonly called the Lackawanna Six) pled guilty to supporting terrorism (May 2003).
- In Detroit, Michigan, two individuals were convicted of conspiring to support Islamic extremists (June 2003).
- In Tampa, Florida, eight individuals were indicted for alleged support of the Palestinian Islamic Jihad (ongoing).
- In Alexandria, Virginia, an Al Qaeda loyalist was charged as an alleged conspirator in attacks of September 11, 2001 (ongoing).

Sources: Senate Report 107-218, Departments of Commerce, Justice, and State, Appropriations Bill, 2003; White House Progress Report on the Global War on Terrorism, September 2003.

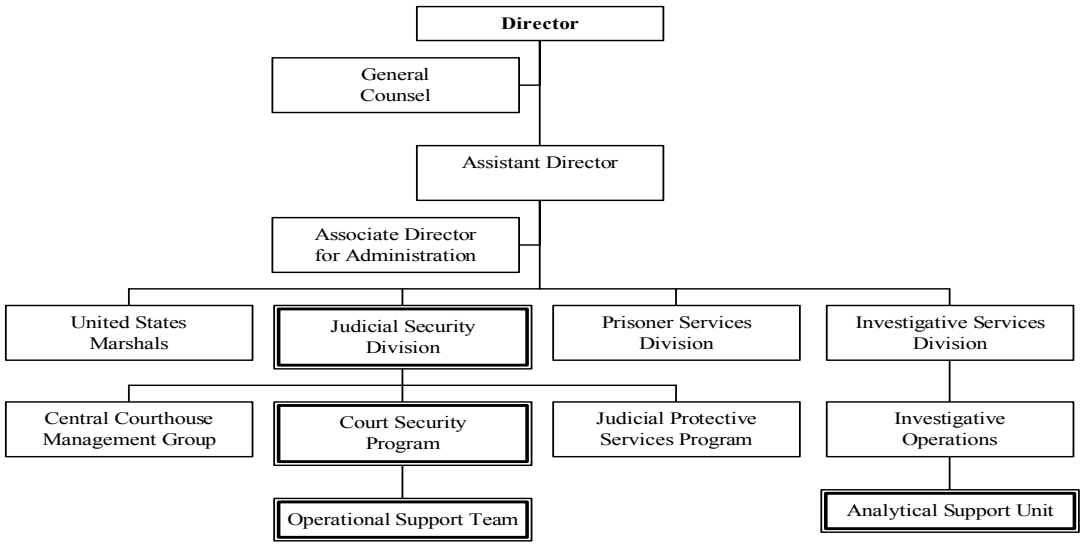
Court Security Program. This program provides operational and administrative support to the 94

[15] Testimony of the Attorney General before the Commerce, Justice, State and Judiciary Subcommittee of the Senate Appropriations Committee on April 1, 2003.

[16] Conference Report 108-10, February 13, 2003, p. 735-736.

[17] The three federal judges assassinated in the last 25 years were away from the courthouse when they were killed (Judge Wood in 1979; Judge Daronco in 1988; and Judge Vance in 1989). All the assassinations were related to cases on the judges' dockets.

Figure 2 - USMS Organization



Source: DOJ Organization and Functions Manual, August 2002.

USMS districts to assist them in protecting the federal judiciary and other officers of the court. The program provides operational and administrative assistance on security for judicial conferences and high-threat trials; security surveys of federal courts and other facilities and some state and local courts; security education programs for federal and state courts; security details for Supreme Court Justices outside the District of Columbia Metropolitan Area; and protective investigations and protective services details for the federal judiciary.

The program is administered by the Operational Support Team (OST), which consists of four Senior Court Security Inspectors (Deputy Marshals) and administrative personnel. Prior to FY 2003, the USMS had 3 Senior Court Security Inspectors assigned to the OST at USMS headquarters and 28 Circuit Court Security Inspectors assigned to the 13 judicial circuit courts across the country. Shortly after September 11, 2001, at the request of the Administrative Office of the United States Courts (AOUSC), Congress provided 106 additional District and Circuit Court Security Inspector

positions.[18] In May 2003, the USMS deployed the 106 Court Security Inspectors to the 94 federal district courts and 12 of the 13 circuit courts.[19]

Judicial Protective Services Program. This program provides about 4,000 contract guards, called Court Security Officers (CSOs), assigned to all federal district courts and circuit courts. The CSO's provide day-to-day security at courthouse entrances and inside the courtroom.

Central Courthouse Management Group. This group works with district personnel, the General Services Administration, and the AOUSC when planning the construction of new federal courthouses and the renovations of existing courthouses.[20] The group also provides security expertise concerning prisoner movements and the safety of detention facilities.

The Analytical Support Unit (ASU)

In addition to JSD, the Analytical Support Unit (ASU) located in the Investigative Services Division (ISD) supports the USMS's judicial security effort. The ASU provides information and investigative support to USMS investigators protecting the judiciary and conducting fugitive investigations. The ASU works with the Social Security Administration, the Department of Defense, Defense Information Systems Agency, the Department of Agriculture, and various high intensity drug trafficking task forces to locate fugitives. The ASU also administers the Warrant Information Network (WIN) and conducts assessments on threats to the federal judiciary.

Warrant Information Network

WIN is the USMS's central law enforcement information system. WIN contains more than 700,000 subjects of USMS fugitive and protective investigations and is used to track the status of all federal warrants to aid in the investigations of all federal fugitives. It is also used to access the National Law Enforcement Telecommunication System (NLETS) and National Crime Information Center (NCIC) systems to obtain criminal record information from other federal, state, local and foreign law enforcement agencies.

Sources: USMS Investigative Operations Manual, April 2003. Report No. 03-03, Office of the Inspector General, November 2002.

[18] AOUSC is the administrative and fiscal component of the federal judiciary.

[19] USMS Headquarters provides the Court Security Inspector for the Court of Appeals for the Federal Circuit.

[20] On February 13, 2003, Congress directed that the USMS "conduct a study with an independent consultant on…the unique relationship between the Federal Judiciary, the U.S. Marshals Service, and the Federal Protective Service in…providing facilities security for the judiciary." (Conference Report to Accompany H.J. Res. 2, House Report 108-10.)

Threats to the Judiciary

The USMS *Policy and Procedures Manual,* August 6, 1993, defines threats as any communications or actions intended to intimidate, impede, or interfere with a member of the judiciary, their staff, or their family. Threats may be direct or may be implied by suspicious behavior, such as stalking or demonstrating unusual or excessive interest in a judge or a judge's family. Threats can be verbal or written, and can be delivered in person, by mail, by telephone, or by e-mail. In some cases, threats may be reported by a third party, such as when an informant tells authorities of a plan to harm a judge. According to the USMS, most threats against judges are made by individuals angry about the outcome of a particular court case in which they, or people they know, were involved.[21]

The USMS requests federal judges and their staffs to report every threat. However, in 1994 the General Accounting Office (GAO) found that almost 25 percent of the judges responding to its survey did not report all or even most of the threats they received to the USMS.[22] Further, in November 2001 a report prepared for the AOUSC concluded that the off-site security program, particularly the reporting of threats, was underutilized by judges.[23] From FY 1998 through FY 2003, the USMS responded to an average of 691 threats to the federal judiciary each year, most of which came from known sources (Table 1).

Table 1 – Threats to the Judiciary FY 1998 through FY 2003

Fiscal Year	Number Reported	Source Unknown	Source Known
1998	790	104 (13%)	686 (87%)
1999	814	109 (13%)	705 (87%)
2000	702	109 (16%)	593 (84%)
2001	690	126 (18%)	564 (82%)
2002	565	101 (18%)	464 (82%)
2003	585	105 (18%)	480 (82%)

Source: USMS

[21] The USMS labels threats to members of the federal judiciary "inappropriate communications." *The USMS Protective Services Program: A Procedural Handbook for Threat Investigators and Supervisors*, January 1999.

[22] "Comprehensive Risk-Based [Federal Judicial Security] Program" Should be Fully Implemented, GAO/GGD-94-112, April 1994.

[23] A Study of the Court Security Program, November 2001 (AOUSC Study).

The USMS also has assigned Deputy Marshals to other Department of Justice components to collect and share information about potential threats to members of the federal judiciary. These include:

- One Deputy Marshal is assigned to the Federal Bureau of Prisons' (BOP) Sacramento Intelligence Unit (SIU) to collect information, monitor high-threat trials, and conduct threat assessments of groups targeted by large-scale arrest operations.[24]

- One Deputy Marshal is assigned to the Drug Enforcement Administration El Paso Intelligence Center (EPIC) to identify any information related to high-threat trials involving drug charges.[25]

- Fifty Deputy Marshals are assigned to 29 of the Federal Bureau of Investigation's (FBI) 56 field office Joint Terrorism Task Forces (JTTFs), and one Deputy Marshal is assigned to the National JTTF (NJTTF). The JTTFs provide access to intelligence on potential terrorist threats and trials of alleged terrorists.[26]

If a USMS representative to one of the above operations identifies a potential threat to the judiciary, the representative forwards the information to the OST and the appropriate districts.

The USMS Response to Threats to the Judiciary

When a threat is reported, a Deputy Marshal conducts a preliminary inquiry to determine the source of the threat and initiate an appropriate response. Unless the inquiry demonstrates the clear absence of significant risk, a protective investigation is initiated. If a threat is initially assessed as

[24] SIU is part of the BOP Intelligence Section, Correctional Services Branch, Correctional Programs Division. It provides operational intelligence and direct investigative support to various field operations.

[25] EPIC collects intelligence on drug movements and immigration violations and can provide real-time information from its own and other federal databases.

[26] The first FBI JTTF was created in 1980. As of November 2003 there were 84 JTTFs operating across the United States. There is one JTTF operating in each of the 56 FBI field offices. Each JTTF includes members from federal, state, and local law enforcement organizations. The JTTFs are intended to enhance the collection and sharing of information and intelligence, and to work on specific FBI domestic and international terrorism investigations. The USMS has formally participated in JTTFs since July 17, 2001, when it entered into a Memorandum of Understanding with the FBI.

likely to be carried out, the USMS will employ a range of interim protective measures to prevent the judge from being harmed.

The districts are responsible for providing the Deputy Marshals, administrative support, and any other resources needed during the first days of a protective services detail. If the protective services detail will take longer than a few days, the districts may request, from the OST, additional staffing and financial resources. The protective services detail ends when the USMS determines that the judge is no longer in danger.

Protective Investigations

"A protective investigation is a process used by the USMS to manage a case to ensure that purveyors of Inappropriate Communications no longer present a threat to the designated protectee. A protective investigation incorporates a range of tactics and strategies designed to identify, diffuse, and manage any potential risk of harm to a protectee. This may include, when appropriate, committing the subject to a mental hospital, obtaining restraining orders, arresting the subject, or maintaining contact with the subject."

Source: "Offsite Security Booklet for Judicial Officers," (USMS Publication 94, March 1999)

The USMS *Policy and Procedures Manual,* August 6, 1993, requires districts to report the result of every preliminary threat investigation and any protective measures taken to the OST in a "Preliminary Threat Report."[27] In addition, districts are required to notify the FBI, which determines if the threat warrants a criminal investigation.[28]

At USMS Headquarters, the preliminary threat report is reviewed by the OST and forwarded to the ASU for an assessment of the legitimacy and seriousness of the threat.[29] USMS Policy Directive 99-07, *Protective Investigations*, January 7, 1999, requires the ASU to complete its assessment and enter the results into the WIN within a specified time period. [30]

[27] The current form used for the report is the USM-550, Preliminary Threat Report (Revised 1/97).

[28] The FBI criminal investigation focuses on collecting evidence that shows a crime was committed. The USMS protective investigation focuses on whether the intent, motive, or ability exists to harm a member of the federal judiciary.

[29] The ASU refers to its part of the threat assessment process as "deliberative analysis." We use the term "assessment" to refer to the entire process and its parts.

[30] USMS Investigative Operations Manual, April 2003. The OIG audited the WIN system in FY 2002. See Audit Report No. 03-03, November 2002.

In conducting its threat assessment, the ASU determines if the threat meets the specific criteria required for the communication or other behavior to be considered a threat. If the criteria are met, and if the identity of the person who made the threat is known, the ASU queries various public and law enforcement databases to determine whether the person has made threats before and if the person has any other law enforcement records.

Next, the ASU conducts a two-step threat assessment. In the first step, the ASU completes a comparative assessment that matches the characteristics of the current threat to threats in its historical threat database to identify prior threats with similar characteristics. The comparative assessment results in a report describing how closely the current threat matches the profiles of past threats with known outcomes. The historical threat database contains information on 3721 threats reported from 1980 to 1996. Each threat is catalogued by up to 30 variables, including the date of the threat, the method of delivery, if the initiator of the threat was identified, his or her motive, and if he or she carried out the threat.[31] Of the threats listed in the historical threat database, no additional action happened after the threat was received in 91 percent of the cases (the USMS terms these types of threats as specious); there was some escalation of activity (such as a suspicious act or an additional communication) in 5 percent of the cases; and the threat resulted in a USMS-defined "violent outcome" (such as an act of vandalism on a judge's property or an attempted physical assault) in 4 percent of the cases (Table 2).

Table 2 - Historical Threat Database Outcomes 1980 to 1996

Outcome	Number	Percent
Specious	3,296	91.02
Enhanced	182	5.03
Violent	143	3.95
Total	**3,621**	**100.00**

Source: USMS (Note: ASU reports that while there are 3,721 threats in the database, only 3,621 have associated outcomes. The remaining 100 cases had no outcome recorded.)

In the second step of the assessment, the ASU examines the threat using a proprietary computer-based threat analysis system. The threat

[31] The USMS stopped entering threat information into the historical threat database in FY 1996 and began entering this data into WIN. However, the data in WIN is not used for automated threat assessment.

analysis system is customized to address the specific needs of the USMS in protecting the federal judiciary by assessing threats using questions about the behavior and background of the threat initiator. The system organizes the details of the current threat and allows the analyst to compare the threat with known outcomes of prior cases.

The assessment results in a rating from one through ten, with higher ratings indicating cases with greater similarity to those in which there is a greater risk that the threat will escalate. Lower ratings indicate that the case has characteristics similar to those that have not escalated, and therefore are considered less serious. Of the 4,297 threats that the USMS assessed using the system through October 31, 2003, about 22 percent received a higher rating (Table 3, next page).

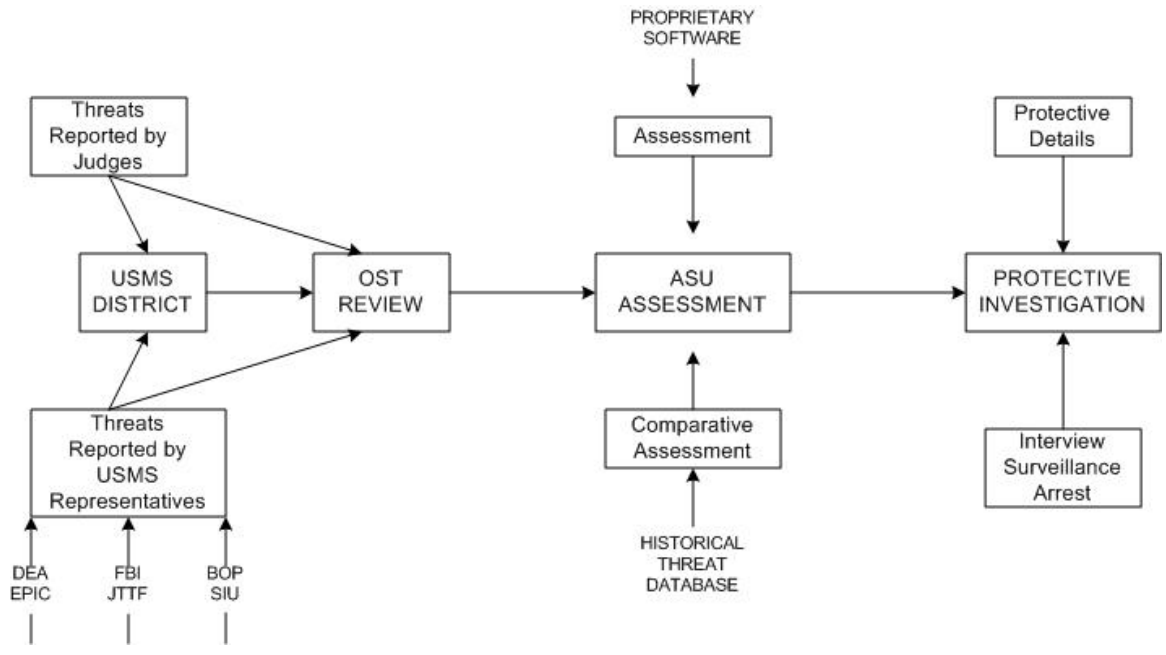
The comparative and threat analysis system assessments should have similar outcomes. If the comparative assessment indicates low risk, then the threat analysis system should indicate low risk as well. When comparative and threat analysis system assessments do not show a similar outcome, the ASU resolves the disparity by requesting additional information from the district to reassess the threat, or provides possible explanations for the disparity to the district. The ASU enters the comparative and threat analysis system assessment results into the WIN.

The district investigating the threat uses assessment results posted in WIN to help determine if adequate protective measures are in place. If a protective investigation is conducted, the WIN record is used by the district and the ASU to track and manage the case as new information is collected and additional investigative work is accomplished. If significant new information is collected, the district can request that the ASU reassess the threat (Figure 3, next page).

Table 3 – Ratings for Threats		
Rating	**Number of Threats**	**Percent**
10	0	0
9	0	0
8	63	1.5
7	324	7.5
6	564	13.1
5	871	20.2
4	1,754	40.9
3	643	15.0
2	72	1.7
1	5	0.1
Total	**4,297**	**100.0**

Source: USMS

Figure 3 - USMS Threat Assessment and Protective Measures



Purpose, Scope, and Methodology

The purpose of this review was to examine the USMS's efforts to ensure the safety of more than 2,000 federal judges and magistrates. We evaluated the USMS's efforts since September 11, 2001, to improve its protection of the federal judiciary. We focused specifically on the USMS's ability to assess threats and determine appropriate measures to protect members of the federal judiciary during high-threat trials and while they are away from the courthouse. We conducted the fieldwork for this review from March 3 through October 18, 2003.

Interviews: We interviewed USMS headquarters officials in the JSD, ISD, and the Office of General Counsel (OGC). We visited and interviewed USMS district officials in the Western District of North Carolina and the Western District of New York to review the security measures associated with recent high-threat trials in those districts. We visited the Southern District of New York for information on high-threat trials and on that district's long-running protective services details for two federal judges who presided over previous terrorist trials. We reviewed USMS files collected on these two long-running protective services details and other protective services details. Substantial portions of those records are classified. For additional information on the threat assessment process, we interviewed officials with the U.S. Capitol Police and the U.S. Secret Service about their respective protective missions.

Databases: We reviewed and analyzed threat data maintained by the ASU, including the historical threat database, computerized threat analysis system, and WIN. We reviewed and analyzed USMS security clearance data provided by its Human Resources Division. We also reviewed records maintained in the USMS's Judicial Protection Information System, which was established "to identify security risks and to develop operating plans and carry out security measures to counteract threat situations" for information related to judicial security.[32]

Surveys: We sent a judicial security survey to all 94 USMS district offices (85 districts responded). We asked the Judicial Security Division (JSD) to conduct a self-assessment and to report post-September 11, 2001, improvements in the judicial security process. The JSD self-assessment appears in Appendix I.

[32] 64 Federal Register 60832, 43, November 8, 1999.

USMS Training: We attended two USMS training sessions on threat assessments and the high-threat trial management process. The first session occurred on April 11, 2003, and involved the threat assessment portion of the Advanced Deputy United States Marshal training. The second session occurred on May 6 and 7, 2003, and involved District and Circuit Court Security Inspector training in San Antonio, Texas.

Additional Resources: The U.S. Capitol Police provided sample documents and other written information regarding its threat assessment process, and the U.S. Secret Service provided copies of several publications and two videotapes on its threat assessment process. In addition, we reviewed the literature generally available regarding the protective services field. We reviewed more than 50 documents, including Departmental publications, articles in professional journals, GAO reports, congressional committee reports and hearing transcripts, and other publicly available congressional information. Among the documents we reviewed were:

- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (March 1983 and the revision dated 2002).

- Strategic Plan, U.S. Department of Justice, Fiscal Years 2001-2006, November 2001.

- Performance & Accountability Report, U.S. Department of Justice FY 2002, January 2003.

- Personal Security Handbook, U.S. Department of Justice, United States Marshals Service, January 1, 2000.

RESULTS OF THE REVIEW

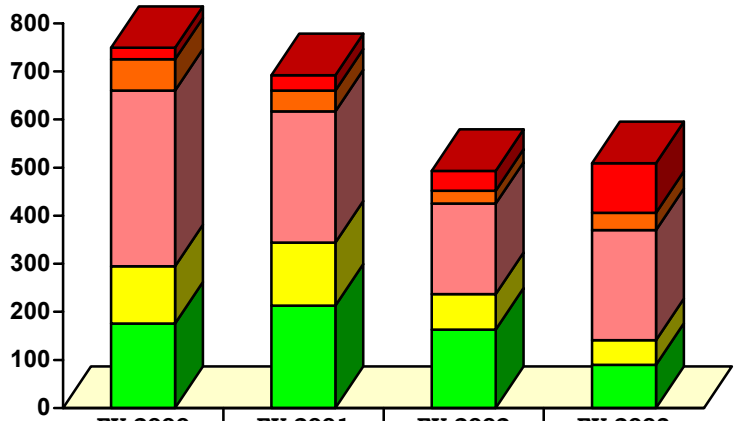
Despite the increased Departmental emphasis on security since September 11, 2001, we found significant shortcomings in the USMS's ability to assess threats, collect and analyze intelligence, and manage judicial protection efforts. The timeliness of the USMS's threat assessments routinely exceeded its internal standard, and often took weeks to complete. The quality of the USMS's assessments is questionable because the assessment process relies on an outdated historical threat database. Moreover, the USMS has failed to act on internal studies conducted since September 11, 2001, that identified the need to improve its capability to collect and share intelligence to assess threats to the federal judiciary. The USMS's shortcomings in quickly and effectively assessing threats, including those associated with terrorist and other high-threat trials, increase the risk that members of the federal judiciary may not be adequately protected.

The USMS Headquarters' Assessments of Reported Threats Routinely Exceed Internal Standard

After two federal judges were assassinated in the late 1980s, the USMS developed a comprehensive system to assess threats and provide protective measures for federal judges. To ensure that threats were rapidly assessed and appropriate protective measures implemented, the USMS established policies and performance standards that require the ASU to assess all threats to the judiciary and post the results in WIN within a specified time period. To evaluate the timeliness of the ASU's assessments, we compared the date that ASU received the threat from the OST and the date that the ASU entered the assessment results in WIN from FY 2000 through FY 2003. We found that only 27 percent of threat assessments were completed within the standard time (Figure 4, next page).

Because threat assessments provide analytical information the JSD uses to allocate additional resources to districts to help them respond to threats when protective services details need to extend beyond a few days, we also examined how many threat assessments the ASU completed within a few days. We found that only 42 percent of the threat assessments were

Figure 4 - Completed ASU Threat Assessments FY 2000 Through FY 2003



	FY 2000	FY 2001	FY 2002	FY 2003
Significantly (Months) Late	24	32	41	103
Several Weeks Late	65	43	27	36
Days to Weeks Late	365	273	188	229
In Local Funding Window	119	131	74	51
Within Standard	176	213	163	90

completed within the time that the USMS allows before additional resources may be provided.

From FY 2000 through FY 2003, the number of threats sent to the ASU for assessment decreased by 30 percent, from 841 cases to 585 cases.[33] Despite the reduced number of threats, the ASU completed fewer assessments within the standard. In FY 2000 the ASU completed 176 cases in less than the standard time, but in FY 2003 it completed only 90 cases within the standard time. The number of cases in which the ASU's assessment was severely late also increased substantially. Specifically, the number of cases in which ASU took several months or more to complete its assessment more than quadrupled, from 24 cases in FY 2000 to 103 cases in FY 2003.

In examining the reasons for the USMS's failure to meet established timeframes, we found that the number of analysts that USMS has dedicated to assessing threats has decreased since the office was established in 1996. The ASU initially was staffed with six analysts, and the number of positions was later reduced to five. When we reviewed the program, only four of the

[33] Although we found no recent studies of judicial reporting of threats, USMS officials told us they believed threats declined, in part, because judges did not report all the threats they received.

five analyst positions were filled. The reduction in staff was compounded by the fact that the analysts perform duties other than conducting threat assessments. The ASU Chief told us that, at any given time, only "two or three" of the four analysts are conducting threat assessments. The analysts spend their remaining time assisting with fugitive cases and working on special projects and reports. Although these other efforts are important, the result is that fewer resources are available for assessing threats to the judiciary.

In response to USMS budget requests, Congress has repeatedly criticized the USMS's failure to hire employees to fill all of the USMS's authorized and funded positions. In response, the USMS told Congress that, in conformance with the Attorney General's direction to fight the war on terrorism by focusing resources on front-line positions, it has held off on filling headquarters positions except on a case-by-case basis.[34] Nonetheless, a 2003 OIG audit noted that the USMS does not track where excess funds are expended.[35] The failure to hire employees to fill positions and the unreconciled reallocation of salary dollars are particularly significant in an organization as small as the ASU, where one position represents 20 percent of the workforce.

ASU's "triage" system for threats does not ensure that the threats the USMS rates as most serious are processed timely. In February 2003, the USMS implemented a new practice under which the OST assigns a rating of high, medium, or low to all threats before forwarding them to the ASU for assessment. The ratings are assigned by an OST senior court security inspector based on his or her expert opinion; there are no written criteria for assigning the ratings. The ASU assesses all threats rated high first, followed by all threats rated medium, and then all threats rated low on a first-in/first-out basis.

We found that the triage system has not ensured that all threats rated "high" are processed in a timely manner. Data from the first eight months of operation under the triage system (February 2003 through September 2003) show that 68 threats were rated "high" for assessment out of a total of 408 threats reported. Yet only 20 of the assessments (37 percent) were completed within the standard time. Of the 48 assessments that took

[34] USMS responses to questions for the record submitted by Congressman Charles H. Taylor, May 13, 2003.

[35] Department of Justice, Office of the Inspector General, *Budget Execution in the United States Marshals Service During Fiscal Years 2002 and 2003*, Report No. 04-02, October 2003.

longer than the standard time, 30 took up to 10 days to complete, and 11 took from 10 days to as long as 47 days to complete.

Moreover, because the formal assessment of threats initially prioritized as "medium" or "low" is delayed, the triage system may have negative effects on the threat assessment process. The lack of written criteria for assigning ratings risks that some serious threats will be rated "medium" or "low," resulting in a delayed assessment. Also, one of the most important factors considered in assessing a threat is determining whether the person has made multiple threats and if the threatening behavior is escalating. The USMS considers these threats to be more serious. If all threats are not processed in a timely manner and in the order they are received, the assessments may not identify that other threats by the same person are pending, and the seriousness of the threat may not be accurately determined.

The USMS's Analysis of Threats Relies on an Outdated Analytical Tool

The database that the USMS uses to perform the comparative assessment on reported threats has not been updated since 1996 and therefore lacks current data on threats (including those involving terrorism) needed to reliably assess reported threats against the federal judiciary. When the ASU conducts a threat assessment, it compares the available information about the current threat and its initiator to information about prior cases contained in the historical threat database. The USMS ceased adding information on threats to the historical threat database in early FY 1996 and began entering threat assessments into WIN. As of September 30, 2003, ASU records showed that a total of 8,694 threats had been reported to the USMS since 1980. However, the historical threat database does not contain any information on 4,973 of those threats that were reported since 1996, including cases involving terrorism after September 11, 2001.

The ASU stopped adding information into the historical threat database because ISD decided that it would be more cost-effective to enter the data into WIN than to update the DOS-based, historical threat database program. In addition, according to the USMS, because many individuals who make threats also have outstanding warrants, entering threat information directly into the WIN system could speed the identification and apprehension of these individuals.[36]

[36] USMS Memorandum from Assistant Director (ISD) to Deputy Director, *Assignment of Analytical Support Unit*, March 11, 2002.

Our analysis of WIN data since June 1996 did not substantiate the USMS's reasoning. We found that only 19 percent (772 of 3,756) of the individuals who made threats also had warrants issued for their arrest. Those 772 warrants represented only about one-sixth of one percent of the 483,983 warrants that were entered into WIN since June 1996. Moreover, the districts and the ASU cannot rely solely on WIN for threat information. Although WIN can be used to collect and share some information regarding threats to the federal judiciary, it was designed to support the USMS fugitive program and has been modified to collect and process only some threat information. For example, WIN provides the summary results of post-1996 threat assessments conducted by ASU but does not contain all of the threat details that were used to conduct the assessment.

While WIN was designed to systematically collect all relevant categories of information on threats in a format that supports the use of the information for future assessments, according to the ASU Chief, the USMS has not added a comparative threat assessment capability to WIN as originally planned. Therefore, although information on threats has been entered into the WIN since FY 1996, the ASU continues to conduct the comparative assessments on new threats using the outdated historical threat database.

The USMS continues to rely on the outdated historical threat database to allocate resources. The USMS's analysis of the historical threat database showed that, of all threats received from 1980 to 1996, 91 percent were "specious" (i.e., nothing further happened), 5 percent resulted in some form of escalation (e.g., additional threats, stalking), and 4 percent resulted in violence (e.g., vandalism of the judge's property or worse). According to Court Security Inspectors assigned to the OST, the USMS continues to allocate resources, including conducting threat assessments and implementing protective measures in response to threats, based on the presumption that only one in ten threats will escalate or result in violence. However, the extent to which the database is outdated casts serious doubt on the validity of that presumption.

In summary, our review showed that the USMS often fails to assess reported threats within its standard time and relies on an outdated assessment tool to assess threats to the federal judiciary. Without timely assessments, the USMS cannot fully identify and assess serious threats to judicial operations and personnel. Further, without any information on recent terrorist-related threats in the historical threat database, the validity of the ASU's comparative assessments for judging the severity of threats against the federal judiciary and identifying appropriate protective measures

is questionable. The USMS's failure to ensure that threat assessments are both timely and based on current and complete data reduces the capability of the USMS to adequately protect the federal judiciary.

The USMS Has Limited Capability to Collect and Assess Intelligence to Identify Potential Threats to the Federal Judiciary

We found several limitations that prevent the USMS from effectively collecting and assessing intelligence from the districts and other sources, such as the FBI's JTTFs, to identify potential threats to the federal judiciary. The USMS's capability to collect and assess intelligence is limited by the lack of a central information collection capability; internal prohibitions on collecting information; incomplete participation in the FBI's JTTFs; insufficient security clearances; and inadequate secure communication systems.

These limitations persist, in part, because since September 11, 2001, the USMS has failed to implement new authority granted by Congress in the Patriot Act, and failed to act on internal studies to improve its information collection and sharing capabilities.

The USMS disbanded its centralized unit that collected, assessed, and shared information on threats to the judiciary, and issued internal guidance that limited information collection. Prior to 1994, the USMS had a formal centralized intelligence collection and assessment program operated by its Threat Analysis Division. However, during a 1994 reorganization of the USMS headquarters, the Director eliminated the Threat Analysis Division. Further, on April 5, 1996, the USMS Office of General Counsel (OGC) issued an opinion that directed the USMS to limit intelligence collection (including information in the databases used to track and assess threats) and threat investigations relating to extremist groups. The 1996 OGC opinion was based on the Attorney General Guidelines issued in 1983 which have been superceded, and cautioned Deputy Marshals that they could be held personally liable for collecting information not directly related to specific threat investigations.[37] After the 1996 OGC memorandum, the USMS dismantled its remaining centralized intelligence capability by destroying all intelligence files not directly related to specific threat investigations.

[37] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (March 1983) described authorities and activities related to criminal investigations. Although the Guidelines only mention the FBI, they have been interpreted as applying to all DOJ criminal investigations.

The ISD Assistant Director told us that currently the USMS headquarters' only threat assessment capability resides with the ASU, but that the ASU is still prohibited from collecting and sharing information not related to specific reported threats. Moreover, even if the current OGC limitations on intelligence collection were removed, the current ASU staff could not provide a centralized information collection and sharing capability because, as described previously, it is unable to meet its current threat assessment workload.

Because the USMS headquarters has no centralized capability to collect and share information not related directly to a specific threat investigation, it must rely on Deputy Marshals in the districts and assigned to other Departmental intelligence operations (e.g., the BOP Sacramento Intelligence Unit, DEA's El Paso Intelligence Center, and the FBI's JTTFs) to collect and share information on potential threats to the federal judiciary. If one of these Deputy Marshals learns of a potential threat to the judiciary, he or she forwards that information to both OST and the appropriate districts. While these actions have some value, the information is not made available to all Deputy Marshals responsible for judicial security or systematically assessed and retained to identify trends and emerging threats. More importantly, we found that the current ad hoc efforts do not always provide threat information to the responsible field offices. For example:

> In March 2003 the Deputy Marshal assigned to the Sacramento Intelligence Unit became aware of a threat made by an individual in Arizona against a judge in New York. The Deputy Marshal notified the Southern District of New York. However, the Arizona district, where the individual who made the threat resided, was not immediately notified due to an administrative oversight. The individual did not carry out his threat, but the delay hindered assessment and mitigation efforts and increased the risk that the judge would be harmed.

The USMS's participation in the JTTFs is limited. According to October 2003 JTTF membership rosters provided by the FBI, the USMS has assigned only 50 Deputy Marshals to represent it on 29 of the 56 FBI field office JTTFs (6 of the Deputy Marshals were assigned by USMS headquarters and 44 were assigned by districts). Moreover, only 25 of the 50 are full-time representatives. The other 25 Deputy Marshals assigned to field office JTTFs, as well as the one Deputy Marshal assigned to represent the USMS on the NJTTF, are part-time representatives.

The USMS had planned to increase JTTF participation by assigning an additional 22 Deputy Marshals to the JTTFs, but was unable to do so. For FY 2003, the USMS requested $2.3 million to fund 22 additional Deputy Marshals to be assigned to field office JTTFs. Congress provided all of the requested funds, but directed that 18 of the new Deputy Marshals be assigned to "districts with the highest priority needs" at a cost of $1.4 million.[38] The USMS complied with the congressional direction regarding the $1.4 million, but an FY 2003 OIG audit could not establish where the USMS allocated the rest of the money.[39]

The USMS JTTF representatives and their supervisors lack appropriate security clearances. In addition to the absence of full-time representatives on many JTTFs, the USMS's ability to access and share JTTF information on threats to the judiciary is also limited by a lack of security clearances. The July 2001 Memorandum of Understanding between the USMS and the FBI requires that Deputy Marshals assigned to a JTTF – as well as their appropriate supervisory personnel – must have Top Secret security clearances verified by the FBI to access JTTF intelligence. However, our review indicated that not all USMS representatives have the security clearances necessary for full access to JTTF intelligence. According to an October 2003 Top Secret clearance roster provided by the USMS, only 33 of the 50 Deputy Marshals listed on FBI JTTF rosters had a Top Secret security clearance.[40]

The lack of appropriate security clearances is not limited to the USMS representatives assigned to the JTTFs. While 92 of the 94 U.S. Marshals have Top Secret clearances, the Chief Deputy Marshals in 22 districts did not have the Top Secret Clearances required to supervise JTTF members or receive or review classified information.[41] Overall, the USMS Top Secret

[38] Senate Report 108-33. The Congressional direction to assign the new Deputies to the "districts with the highest priority needs" did not preclude additional full time participation in the JTTFs.

[39] Department of Justice, Office of the Inspector General, *Budget Execution in the United States Marshals Service During Fiscal Years 2002 and 2003*, Report No. 04-02, October 2003.

[40] USMS Human Resources Division, Top Secret Security Clearance Roster compiled for OIG, dated October 22, 2003.

[41] Every district has a Chief Deputy Marshal who provides the overall day-to-day supervision of the Deputy Marshals assigned to that district.

clearance roster showed that only 876 of 4,761 USMS employees (17 percent), only 696 of 3,342 Deputy Marshals (16 percent), and only 26 of 106 of the recently assigned District and Circuit Court Security Inspectors (25 percent) possess a Top Secret clearance. In response to our survey, 25 of 85 responding USMS districts (29 percent) reported that they did not have any Deputy Marshals with a Top Secret clearance.

Further, some intelligence information has additional restrictions and requires a special authorization in addition to a Top Secret clearance for access. As the Joint Committee on Select Intelligence Inquiry concluded, "without [Sensitive Compartmented Information] clearances, non-intelligence community agencies are often unable to access vital counter-terrorism information."[42] However, few USMS personnel have the additional authorizations to access Sensitive Compartmented Information. As of June 2003, only 144 USMS employees (3 percent) were authorized to access Sensitive Compartmented Information. Of those 144 individuals, 26 were assigned to just one district where a high-threat trial was underway.

According to the Chairman of the USMS Executive Working Group tasked by the Director to examine USMS intelligence capabilities, the wide-spread lack of clearances at all levels represents a barrier to improving intelligence collection and sharing. In the two cases we looked at, we found that the USMS's lack of effective participation in JTTFs negatively impacted the USMS's ability to provide appropriate security to the federal judiciary.

One intelligence-sharing breakdown occurred during a JTTF investigation of a terrorist cell. Arrests were imminent and, once the suspected terrorists were arrested, the USMS would be responsible for transporting and housing them, as well as for providing courtroom security. However, the responsible USMS district (which did not have a representative on the JTTF) was unaware of the investigation or the impending arrests until a few hours before they took place. This short notice precluded adequate planning for the extensive security measures needed to handle a large number of suspected terrorist prisoners.

The other case occurred during a high-threat trial that involved individuals who were accused (and subsequently convicted) of providing financial aid to terrorists. In that case, classified information that the district later considered critical to trial security was not disclosed to the

[42] Statement of Eleanor Hill, Staff Director, Joint Inquiry Staff, to the Joint Select Committee on Intelligence, October 1, 2002.

USMS by the JTTF during the trial because the District's part-time representative to the JTTF did not have a Top Secret security clearance.

The USMS lacks the secure systems needed for Deputy Marshals to effectively share intelligence on threats to the judiciary. As of August 20, 2003, the USMS reported that only 51 of the 94 districts had the necessary secure communications equipment to effectively share classified information.[43] In comparison, the U.S. Secret Service and the FBI indicated that they have fully implemented secure communications systems for sharing classified information and are working to further improve this capability.[44]

Further, threat information is contained in automated and manual systems maintained by individual districts, the JSD, and the ISD. The current systems do not interact to provide the USMS with a secure electronic information system that it needs to enable Deputy Marshals to collect and share threat information among all USMS districts. For example, to test the utility of the current USMS system of records for conducting threat investigations, we obtained information on two protective services details that the USMS currently has underway in the Southern District of New York. We found the information regarding the protective services details in several places, including WIN; historical budget records and operational plans from JSD manual records; current budget and operations plans from the district; and classified material maintained by JSD and ISD. A Deputy Marshal assessing a threat would be faced with the need to collect information from a variety of sources.

The USMS has taken only limited action to improve its information collection and sharing capabilities after September 11, 2001. After September 11, 2001, Congress passed the Patriot Act, which clarified the authority of federal agencies to collect intelligence and law enforcement information.[45] Subsequently, the Attorney General Guidelines were revised to support law enforcement agencies' use of new powers relating to information collection and criminal procedures to more aggressively pursue

[43] During this review, the USMS was contemplating plans to deploy secure communications equipment to an additional 23 Districts.

[44] Targeted Violence Information-Sharing System (TAVISS) Feasibility Study, May 2002.

[45] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [Patriot Act], Public Law 107-56, October 25, 2001.

potential criminal activity especially as it relates to terrorism.[46] However, the USMS has not revised its internal guidance (i.e., the 1996 OGC opinion) to improve the collection and sharing of information on threats to the federal judiciary.

In addition, internal USMS studies conducted after September 11, 2001, identified the need for better information sharing. In September 2001, the Deputy Director of the USMS directed the Assistant Director in charge of the ISD to lead an Executive Working Group to examine the USMS's "capabilities with regard to the collection, analysis, maintenance, and dissemination of information and/or intelligence related material that impacts our criminal investigations and protective operations missions."[47] A White Paper prepared in February 2003 for the Executive Working Group and other senior USMS staff described the limited USMS intelligence capabilities and the need for a centralized intelligence capability and better intelligence sharing, and concluded that the USMS "has no formal process to assess and disseminate information…to prepare for threats or to… participate fully in intelligence sharing."

A "Needs Assessment" prepared for the USMS Director in July 2002 identified a three-phase plan to catalog existing information resources, identify new resources, and develop a centralized information sharing program. The proposal envisioned a staff of 18. The program would collect information from the districts, USMS representatives on JTTFs, and USMS liaisons that would be assigned to the intelligence units of other agencies, including the Central Intelligence Agency, the Foreign Terrorist Tracking Task Force, the Secret Service Protective Intelligence Division, and others. The key goal of the new USMS unit would be to "fuse" information from across mission areas. To date, this program has not been implemented.

In summary, as of October 2003, the USMS has not taken basic steps to ensure that it has access to the information it needs to accomplish its judicial protection mission. To meet its responsibility to the federal judiciary, the USMS needs a centralized information sharing program to collect and share intelligence in order prevent acts of violence. Currently, two trial judges are under express death threats from terrorist groups, and other trials involving similar terrorist groups are underway. Despite the recognized importance of developing JTTF protective intelligence to support

[46] The revised Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, were issued on May 30, 2002.

[47] September 2001 Tasking Statement for the USMS Executive Working Group.

the USMS mission, including the expressed interest of the Congress in the USMS's participation in the JTTFs, the USMS has not established complete participation in all of the FBI's JTTFs. Without a structured, centralized intelligence process; the necessary Top Secret clearances; and the technology to facilitate intelligence sharing, the USMS cannot effectively access and use JTTF intelligence or other intelligence sources to identify potential threats to the federal judiciary.

The USMS lacks adequate standards to guide the selection, adjustment, and termination of measures to protect the judiciary against assessed threats of varying risk (i.e., risk-based standards). In particular, current USMS policies provide no criteria to ensure that protective measures implemented on terrorist and other high-threat trials are appropriate to mitigate the assessed risks. Also, current USMS policies on the application, duration, or termination of protective services details to guard threatened judges are outdated. Consequently, USMS districts select protective measures for high-threat trials and determine the extent and duration of protective services details on an ad hoc basis. The absence of risk-based standards results in inconsistent protection and prevents the USMS from effectively allocating resources among all assessed threats.

The USMS Lacks Adequate Risk-Based Standards for Determining Protective Measures on Terrorist and Other High-Threat Trials

The USMS Policy and Procedures Manual (Manual) provides limited and outdated guidance for determining appropriate protective measures for high-threat trials. The chapter of the Manual that contains guidance and standards for judicial and court security, Volume X, has not been revised since July 1, 1993, and does not address protective measures to be applied when providing security on terrorist and other high-threat trials.[48] For example, ten U.S Marshals and Deputy Marshals that we interviewed noted that the guidance in the Manual does not address many types of trials that present significant risks to the judiciary, such as criminal cases involving espionage, prosecutions of gang violence, and cases with cooperating witnesses. Moreover, a significant defining issue in recent high-threat trials – that the defendants are associated with international terrorist groups – is not included.

Our review of the Manual confirmed that it provides limited and inadequate guidance on determining protective measures on high-threat trials. For example:

[48] Some other parts of the Manual were revised in 1995.

- To determine protective measures for trials, the Manual instructs Deputy Marshals to use several rudimentary "risk matrices" to categorize civil and criminal trials into risk levels according to the subject of the proceeding (e.g., bankruptcy, deportation, assault, narcotics), the stage of the proceeding (i.e., pre-trial, trial, post-trial), and the perceived risk associated with the trial participants. Based on the risk level derived from the matrices, the Manual directs the staffing that should be applied to the trial. Other than dictating the number of Deputy Marshals required, the Manual provides no guidance on protective measures for high-risk trials.

- For trials that the Manual defines as "sensitive," the Manual instructs the U.S. Marshal to prepare a written Operational Plan that will describe the security measures to be implemented and the staffing that will be provided.[49] However, the Manual provides no guidance and establishes no standards that the U.S. Marshal can use to select the protective measures that are the most appropriate and effective for the identified risks. Specifically, the Manual provides no guidance when to request support from the USMS's Special Operations Group (SOG) or Hazardous Response Unit, and establishes no standards for the application of such protective measures as trace explosive detectors, armored cars, body armor, and enhanced prisoner restraints.[50]

Almost half of the USMS districts we surveyed identified the protective measures described above as valuable technology for ensuring judicial security. However, in the absence of adequate guidance and risk-based standards to ensure that appropriate protective measures are selected, the U.S. Marshals cannot ensure that the protective measures chosen are consistent with successful approaches applied in similar circumstances. Consequently, we found that, although districts developed the Operational

[49] The Manual defines "sensitive" trials as those that require non-routine security measures, such as trials with multiple defendants, defendants who are dangerous or may attempt to escape, or where there is high media interest. The term "high-threat trial" equates to "sensitive trial."

[50] The Special Operations Group is a specially trained and equipped unit deployed in high-risk law enforcement situations. USMS Policy Directive No. 99-17, May 24, 1999. The Hazardous Response Unit is trained and equipped for chemical, biological, radiological, nuclear, and explosive device response in relation to high-threat terrorist trials. USMS responses to questions for the record submitted by Congressman Charles H. Taylor, May 13, 2003.

Plans required by the Manual, they did not consistently apply similar protective measures in response to similar threats. For example:

- One district we visited used the SOG extensively to transport prisoners and as a rapid response force during a high-threat trial. Another district did not use the SOG at all for a similar high-threat trial. Neither district could provide any criteria to explain their decision to request (or not to request) that the SOG be deployed.

- The Manual states that personal electronic devices may be banned from the courthouse or the courtroom during some "sensitive" trials. However, after recent intelligence and media reports of terrorists using electronic devices as improvised bomb detonators, we found some USMS districts have worked with the Chief Judge of their districts to make the prohibition on electronic devices permanent while others have not.

- Another district we visited did not use its new "Itemiser^3 Trace Explosive Detector" during a high-threat trial because the district was waiting for guidance from USMS headquarters on where to deploy the equipment (public or freight entrance), who should be screened, and what protective measures should be taken if suspected explosives are detected (e.g., retest for false positive or immediately evacuate the building).

Although specific protective measures must be selected based on the characteristics and risks of each individual trial or threat, the inconsistent approaches used in the field were not readily apparent to the USMS because it does not complete after-action reports on the protective measures taken. Without effective and current standards, and routine after-action reports, the USMS cannot identify inconsistent protections, needed improvements, or successful protective measures for ensuring the security of the federal judiciary.

The lack of adequate standards for protective measures during high-threat trials also prevents the USMS from ensuring that the districts are consistently provided additional resources to support appropriate protections. The USMS could not identify how many high-threat trials have taken place because USMS headquarters (specifically the JSD) only keeps records on high-threat trials for which it provides additional funding. The JSD does not track requests that are rejected, and USMS districts are not required to track or report the number of high-threat trials that occur.

In our survey, we requested that each USMS district estimate the percentage of trials that it perceived as involving increased risk. The responses we received (from 85 districts) indicated that about 20 percent of trials involved a "substantial potential for violence." According to the AOUSC, 12,817 trials were completed in U.S. District Courts in FY 2002.[51] Extrapolating from the districts' responses to our survey, the number of trials with "substantial" risks could have exceeded 2,400. In contrast, JSD records from the last three fiscal years show that JSD provided support for an average of only 139 trials each year (Table 4). Without adequate risk-based standards, and without after-action reports to evaluate and improve its protection of the judiciary, the USMS cannot effectively ensure that the most significant risks are addressed and that its resources are used appropriately.

Table 4 – JSD Funded High-Threat Trials

Fiscal Year	Number of "High-Threat Trials" Funded
2001	139
2002	117
2003	162

Source: JSD

USMS Guidance on Protective Services Details is Outdated

When a protective investigation indicates that an individual may carry out a threat, and interventions such as the arrest or commitment of the individual for psychiatric observation are not feasible, the USMS district can implement increased personal protective measures to protect the threatened judge away from the court building. The USMS refers to these off-site protective measures, which can range from an escort to and from work to around-the-clock protection for the judge and his family, as "protective services details."

The USMS's guidance for protective services details is contained in its Policy and Procedures Manual, Volume X, January 1993, and in USMS Policy Directive 99-07, January 7, 1999, Protective Investigations.

[51] AOUSC FY 2002 Annual Report, Table C-7, U.S. District Courts – Civil and Criminal Trials Completed.

The Manual and Policy Directive are supplemented by *The U.S. Marshals Service Protective Investigations Program, A Procedural Handbook for Threat Investigators and Supervisors*, January 1999. Although our survey of USMS districts indicated that the use of protective services details has increased since September 11, 2001, the USMS guidance has not been updated.

In FY 2002, JSD provided resources for 21 protective services details, several of which included around-the-clock protection.[52] The JSD only tracks protective services details for which it provides resources or expert advice. It does not track the total number of protective services details that are implemented throughout the USMS. In our survey, 71 of the 85 districts (84 percent) reported that they had used protective services details. Of those 71 districts, 14 (20 percent) reported that they had increased the use of protective services details since September 11, 2001. Despite the reported increasing use, we found that the USMS guidance on protective details has not been revised and contains outdated information. For example:

- Neither the Manual nor the Policy address the use of technology during protective services details. For example, the U.S. Marshals and Deputy Marshals we interviewed and surveyed indicated that equipment that has become more widely available in recent years, such as cellular phones, car alarms, and home alarms, might be effective for improving off-site judicial security.

- The Manual states that protective services details will be terminated at the protectee's request or if the Chief of the Court Security Division with the assistance of the Threat Analysis Division determines the protectee is no longer in danger. This standard does not take into account threats by terrorists and similar groups with worldwide reach and a long-term dedication to revenge. Such threats cannot be identified and assessed by the USMS alone. Instead, the threat posed by terrorist groups may require long-running personal protective measures, based on classified intelligence, to safeguard the judges and other participants from reprisal long after the actual trial has ended.

- The Manual has not been updated to reflect that the Threat Analysis Division was disbanded in 1994, and that the Division's mission was not reassigned to any other office. We confirmed that

[52] Judicial Security Division 2002 Annual Report.

the functions and authority of the Threat Analysis Division to "determine if the [protective services] detail is to be continued or expanded" have not been reassigned.[53]

As with the application of security measures for high-threat trials, in the absence of clear standards, the districts we visited did not use a consistent approach for deciding when to implement protective services details or its makeup. The districts we visited could identify no specific criteria for determining the nature and extent of the protections they employed in each case. We also found that two individual protective services details on different judges were maintained while they were both inside the same secure courthouse, unnecessarily duplicating the protective coverage.

[53] We also found that the *Offsite Security Booklet for Judicial Officers* (USMS Pub. No. 94, March 1999), currently provided to members of the federal judiciary to explain the USMS's judicial protection procedures, contains the same out-of-date information regarding protective services details. The booklet informs members of the federal judiciary that the "U.S. Marshals Service Threat Analysis Division will verify all facts and determine if the [protective] detail is to be continued or expanded."

CONCLUSIONS AND RECOMMENDATIONS

Since September 11, 2001, the USMS has placed greater emphasis on judicial security, but it faces significant challenges in its ability to assess threats and determine appropriate measures to protect members of the federal judiciary. Our review found that that the USMS fails to assess the majority of reported threats against the judiciary in a timely manner. Since FY 2000, over 70 percent of the assessments were not completed within the USMS's required timeframe. Additionally, over 55 percent were not completed within the time that USMS allows before additional resources may be provided, and almost 15 percent took weeks to months to complete. The lack of timely assessments impacts the districts ability to determine if appropriate investigative and protective measures have been taken. Also, no new threat information has been entered into the historical threat database used to assess new threats since 1996. The lack of current threat information in the database undermines the validity of new assessments both for determining appropriate protective measures and for allocating resources.

Further, the USMS has limited capability to collect and share intelligence on potential threats to the judiciary from USMS districts, the FBI's JTTFs, and other sources. While the USMS has taken some steps since September 11, 2001, to evaluate its capability to collect and share threat information, it continues to lack an effective intelligence program designed to collect, analyze, and disseminate intelligence related to high-threat trials and threats to the federal judiciary. Without a structured, centralized intelligence program, the necessary Top Secret clearances, and the technology needed to facilitate information sharing, the USMS's capability to share and effectively use information obtained from internal sources and external entities to protect the federal judiciary is limited.

The USMS also needs current risk-based standards for determining the appropriate protective measures that should be applied to protect the judiciary during high-threat trials and protective services details. Risk-based standards also are needed to more effectively identify those high-threat trials for which the districts should receive additional resources. Without current risk-based standards for high-threat trials and protective services details, the USMS cannot effectively ensure that the most significant risks to members of the federal judiciary are addressed and that resources are used appropriately. Finally, the USMS does not complete after-action reports on high-threat trials and protective services details, and

so cannot determine if protective measures were appropriate, and cannot effectively evaluate and improve its protection of the federal judiciary.

The USMS has a responsibility to meet the increasing security needs of the federal judiciary. Congress has supported security improvements by substantially increasing funding for the USMS judicial security mission, even though it has expressed concern that the USMS has not given sufficient attention to the judicial security program. Our review concluded that, to successfully meet the strategic goal of the Department to protect the judiciary, the USMS must improve its ability to assess threats in an accurate and timely manner, and develop a proactive approach to collecting and sharing the information necessary to meet increasing security challenges.

Recommendations

To improve the USMS's capacity to carry out its primary mission of protecting the federal judiciary, we recommend that the USMS take the following actions:

1. Ensure that all threats to the judiciary are assessed within established timeframes.

2. Update the historical threat database or develop a new database to perform comparative assessments.

3. Assign full-time representatives to all 56 FBI field office JTTFs and ensure effective USMS liaison with intelligence agencies (e.g., the U.S. Secret Service's National Threat Assessment Center, the Central Intelligence Agency, and the National Security Agency).

4. Create a centralized capability to identify, collect, analyze, and share intelligence with USMS districts, as well as with the USMS JTTF representatives and other intelligence liaisons.

5. Require that Chief Deputy Marshals and USMS JTTF representatives have Top Secret clearances, and ensure that each district has secure communication equipment.

6. Revise the 1993 *Judicial and Court Security Manual* and the 1999 *Offsite Security Booklet for Judicial Officers* to establish risk-based standards and require after-action reports for high-threat trials and protective details.

APPENDIX I: USMS JUDICIAL SECURITY IMPROVEMENTS

The following security enhancements have been placed into effect post 9/11 by the Judicial Security Division:

Operation Support Team:

- Added one additional Senior Inspector to the Duty Desk.
- Discontinued Level one security for judicial conferences (Levels 2 through 4 in use).
- Conducted two Protective Investigations Training sessions one in FY 2002 and one in FY 2003.
- All federal courthouses have been operating at Security Level 3 or higher since September 11th.
- 105 new District/Circuit Court Security Inspectors have been hired and trained.
- Arrangements were made with the U.S. military to provide emergency evacuation of federal judges from judicial conferences (and potentially other scenarios).

Judicial Protective Services:

- Rapid staffing of 358 Temporary CSO positions nationwide following the traumatic event of September 11th. These positions continue to be programmed for funding.
- Directed the purchase and enhancement of protective vests for all CSOs.
- Developed an on-line Internet application of the CSO Resource Call

(budget request), reducing the number of hours and paper associated with calculating CSO staffing resource requirements, both on the district and headquarters levels.

- Post September 11th, 577 CSOs have been trained.

- Coordinated the finalization of the Memorandum of Understanding (MOU) between the Administrative Office of the U.S. Courts and the USMS, regarding the staffing of the new 105 District/Circuit Court Security Inspectors, to include a desktop reference center through the intranet to provide field operations guidance and program policy.

Judicial Security Systems:

- Procured 311 state-of-the-art x-ray machines, each including Threat Image Projection software.

- Procured and deployed 175 trace explosive detectors (Itemiser3) at primary courthouses nationwide. Arranged for initial on-site training of U.S. Marshals Service personnel and Court Security Officers (CSO).

- Accelerated by one year the upgrade of all CSO radio equipment to the new national standard for digital, encryption-capable units.

- Designed and procured construction and security equipment installation services for upgrades to courthouse perimeters at 141 sites.

APPENDIX II: THE USMS'S RESPONSE

U.S. Department of Justice

United States Marshals Service

Office of the Director

Washington, DC 20530-1000

February 4, 2004

MEMORANDUM TO: Glenn Fine
Inspector General

FROM: Benigno G. Reyna
Director

SUBJECT Review of the United States Marshals Service Judicial Security Process, Assignment Number A-2003-006

Thank you for the opportunity to comment on the draft report for the Review of the United States Marshals Service Judicial Security Process. Each recommendation has been addressed in Attachment 1. For clarification of certain issues raised in the body of the report, but not incorporated in the recommendations, additional commentary (Attachment 2) follows our proposed corrective actions. Please consider the entire attachment our response to the subject draft report.

Should you have any questions or concerns regarding this response, please contact Isabel Howell, Audit Liaison, at 202-307-9744.

Attachment 1: Proposed Corrective Actions
2: Additional Clarification/Commentary

cc: Paul A. Price
Assistant Inspector General for
Evaluation and Inspections
Office of the Inspector General, DOJ

Sylvester Jones
Assistant Director
Judicial Security Division, USMS

Robert Finan
Assistant Director
Investigative Services Division, USMS

Suzanne Smith
Assistant Director
Human Resources Division, USMS

Gerald Auerbach
Acting General Counsel, USMS

Edward Dolan
Chief Financial Officer, USMS

Diane Litman
Acting Chief Information Officer, USMS

Vickie L. Sloane
DOJ Audit Liaison

Response to Draft Report A-2003-006
Review of the United States Marshals Service Judicial Security Process

INTRODUCTION:

Judicial Security has been the highest priority of the U.S. Marshals Service (USMS) for nearly 215 years. During the years leading up to the tragic events of 9/11, the USMS successfully secured thousands of high risk trials involving foreign and domestic terrorists, drug king pins, Mafia bosses, outlaw motorcycle gangs, and other defendants with long histories of violence. During this same period, the USMS successfully managed numerous trials of high profile public figures whose cases created their own unique set of security risks. None of these trials were disrupted and none of the court family involved were injured.

In spite of this impressive record of success, the USMS renewed and strengthened its commitment to protecting the Judiciary following 9/11. Essentially all management initiatives since 9/11 were designed to enhance an already strong Judicial Security program. These initiatives often taxed the USMS's resources and required the direct participation of hundreds of managers and employees at all levels of the organization. While some of the these accomplishments are appended to the draft report, many are omitted. Some significant examples include:

- Since September 11th, 807 Deputy U.S. Marshals (GS-082) have been hired and trained. The primary responsibility of these employees is Judicial Security. This initiative has been the largest USMS recruitment and training drive in more than 40 years. In addition to greatly enhancing the USMS Judicial Security program, this initiative resulted in the lowest overall vacancy rate in more than a decade. By the end of FY -2003 the USMS was at 99 per cent of its position ceiling.

- Since September 11th, more than 800 Automated External Defibrillators have been deployed in 432 judicial facilities and approximately 300 USMS employees have been trained in their use.

- Since September 11th, approximately 100 USMS employees have been trained as threat investigators. The USMS also established a cadre of highly trained employees who can respond to virtually any chemical, biological, radiological, or explosive threat. They have the training and specialized equipment to detect and mitigate such threats.

- Since September 11th the entire Court Security Officer workforce of more than 4000 has been equipped with and trained on the use of high capacity Glock semi-automatic handguns.

Accomplishments like these have further enhanced the Judicial Security program's reputation as one of the best in the world. We are currently providing Judicial Security Training to hundreds of Colombian nationals and may soon be called upon to provide this training to other countries as well. In addition, the USMS regularly conducts Judicial Security training for state and local law enforcement agencies at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. There is usually a waiting list of state and local officers who want to attend this training.

DRAFT REPORT OVERVIEW:

The draft report is not required to include all the significant Judicial Security accomplishments, nor is it required to provide complete context for its comments and recommendations. Nonetheless, the USMS believes context of the draft report leaves an inaccurate, or at least, incomplete picture. This is further compounded by the use of anecdotal and/or incomplete information. While the draft report contains many examples of this deficiency, a brief sampling illustrates the problem:

Beginning on the third line of the Executive Summary, the draft report says:

> "No federal judges have been assassinated since 1989, but two federal judges have been assaulted in the last three years, and the USMS receives almost 700 threats against members of the judiciary each year."

The USMS believes that this statement totally misrepresents the effectiveness of its Judicial Security program. While a single assault or assassination is unacceptable, the full picture actually supports, rather than questions, the USMS' s capabilities. In the 215 year history of the Federal Judiciary, four judges have been assassinated. The two most recent assassinations occurred in 1988 and 1989. Neither of the judges had been threatened by their assassins and the murders occurred at their homes. The third most recent assassination occurred in 1975. In that case, the Judge was killed after he decided to terminate the security arrangements that had been put in place by the USMS. In none of these cases were the alleged USMS shortcomings mentioned in the draft report the causation factor.

Since September 11th, the USMS has produced prisoners, many of whom were extremely violent, before judges and magistrates over one million times. During this staggering number of occasions when the USMS could have failed in its obligation to protect the judiciary, no judge was ever injured. In addition, the USMS believes that one of the two incidents mentioned in the draft report was actually a random street robbery that had nothing to do with the judge's identity or duties.

Further the Executive Summary states,

> "Since fiscal year (FY) 2001, Congress has increased funding for judicial security by about 50 percent and authorized the USMS to hire 106 new Court Security Inspectors. However, Congress has expressed concern that "as the program has grown sufficient attention has not been provided to program and budget administration."

The draft report never fully explains what the concern actually was and whether or not it was validated. In addition, since the draft report focus is solely on the USMS's ability to analyze threats and its ability to protect the judiciary, a reader could easily assume that Congress's concern was related. First, Congress was concerned that the USMS was not using Judicial Security funding as it had been "earmarked" in the appropriation. A review by the Department of Justice Office of the Inspector General failed to find a single case where the USMS spent these funds other than as Congress intended.

Second, none of the funds appropriated by Congress were "earmarked" for positions to collect or analyze intelligence. If the USMS had diverted funds for this purpose it would have ignored the intent of Congress and violated the well established re-programming requirements.

On page 24, paragraph 3, of the draft report, it says "two trial judges are under express death threats from terrorists groups." Given the repeated allegations of shortcomings in the USMS's ability to analyze threats and protect the judiciary, this is an extremely serious statement. First, the USMS has no information that any judge is under such a threat. Second, those judges who are at increased risk as a result of their participation in terrorist trials have the highest levels of security possible. In fact, their security arrangements are comparable in many ways to those provided to other government officials requiring protection. In some cases these measures are extended to family members. Due to the security sensitivity of these cases, it is not possible to provide more detailed information in this forum.

On page 14, the summary states:

> "The USMS's shortcomings in quickly and effectively assessing threats, including those associated with terrorist and other high-threat trials, increase the risk that members of the federal judiciary may not be protected."

Once again, given the overall tenor of the draft report, this is a very serious observation. ill addition, on page 29, the draft report estimates that more than 2,400 trials were held in an environment of "substantial" risk during Fiscal Year 2002 and that ". . . the USMS cannot effectively ensure that the most significant risks are addressed and that its resources are used

appropriately." However, the draft report does not mention that no trial has been disrupted and no judge, juror, witness, or prosecutor, has been injured since September 11th. Given these facts, it is not clear upon what information these statements in the draft report are made.

The most troubling example is the summary at the top of page 26. It suggests that the USMS Judicial Protection techniques are not "adequate" or "appropriate." It further alleges that "outdated" policies cause protective measure decisions to be made in an "ad hoc" and "inconsistent" manner. Finally, it tells the reader that the USMS is not able to "effectively allocate resources among all threats." According to the draft report, these USMS deficiencies are primarily due to older policies and a lack of risk-based standards that can be used to determine security requirements and resource allocations. These statements are made without a single example of when these alleged inadequacies resulted in a trial being disrupted or a member of the judicial family being injured.

The summary and narrative that continues through page 31 fail to demonstrate an even basic understanding of how the USMS Judicial Security process works. The requirements for every high threat trial are determined on a case-by-case basis after considering all available information about the case, the instructions from the trial judge, physical characteristics of the courthouse and available resources. Local and/or national Judicial Security specialists and managers develop an operational plan that is tailored specifically to the trial at hand. After sharing the plan with the trial judge and the prosecutor, it is modified as necessary. As the trial unfolds, the operational plan is frequently amended to meet changing conditions. The plans are implemented by personnel who have received specialized training and who utilize the latest in high tech security equipment.

This section of the draft report can also leave the impression that some high-risk trials go without the necessary resources, while resources are wasted on others. The draft report does not mention that 94 per cent of all requests for special assignment resources are approved, nor does it provide any examples of where resource decisions caused disruption or injury. In addition, the draft report provides no factual information or expert analysis of the risks involved to support the statement that "two different protective service details on different judges were maintained while they were both inside the secure courthouse unnecessarily duplicating the protective coverage."

RECOMMENDATION 1: Ensure that all threats to the judiciary are assessed within established time frames.

USMS Comments:

The USMS agrees that all threats should be assessed according to policy. However, it appears from the narrative supporting this and other recommendations in the draft report that the process through which the USMS responds to potential threats was not fully understood. As a

result, the following general description is provided to correct any misunderstandings and clarify the record.

It is the policy of the USMS to encourage all members of the judicial family and their staffs to report any inappropriate communications (IC) immediately. While the USMS believes that this advice is generally followed, it obviously cannot force compliance. When a district is notified of an IC, a trained district threat investigator conducts an immediate assessment to determine if the IC constitutes an imminent and viable threat.

If there is any reason to believe that the IC constitutes a viable threat, district staff, based on their specialized security training and experience, can immediately implement whatever protective measures they deem necessary to mitigate the threat. Protective measures can include every option up to and including XXXXXXXXXXXXXXXXXXXX for the protectee and his/her family. The district can implement these measures for XXXXXXXX without approval from Headquarters and without concern for long-term funding.

Concurrently, the district notifies the Operations Support Team (OST) at Headquarters of the IC and of what steps it has taken to mitigate any potential threats. The district may also alert the FBI of the potential need for a criminal investigation. At this point. the OST determines whether or not to send the IC to the Analytical Support Unit (ASU) for further analysis. If the ASU conducts an analysis. it becomes a factor considered by the OST and the district in determining what steps should be taken next. Further actions may include canceling or increasing protective measures, initiating a full scale protective investigation, seeking court orders governing the conduct of the trial, and determining if the district will require additional resources. It should be noted that if a full scale protective investigation is initiated, it could take months to complete due to its complexity.

We also stress that both the district and the OST personnel have the training, experience, and authority to implement protective measures without a completed analysis from the ASU. In addition, there is nothing in USMS policy or practice to suggest that protective measures would ever be delayed while awaiting the completion of an ASU analysis. Once protective measures have been put in place (XXXXXXXXXXXXXXXXXXXXXX), they are never removed without first discussing the risk level with the protectee and a thorough review by the OST.

USMS Corrective Action:

The USMS will be revising its policy on time frames for the ASU to complete assessments. The new policy will establish criteria that categorize requests according to urgency. Once the policy is implemented, adherence to the time frames will be made a factor in the annual performance evaluations of the ASU staff. The USMS estimates that the new policy will be

implemented by the end of August 2004. The USMS will also review the workload of the ASU and will request additional resources during the FY-2006 budget process if necessary.

RECOMMENDATION 2: Update the historical threat database or develop a new database to perform comparative assessments.

USMS Comments:

The USMS agrees that the threat database should have been updated. In addition, the USMS believes that the threat database is a valuable part of the overall threat assessment and response process. However, the USMS believes that the draft report greatly overstates the role of the database and adverse impact of not having it current.

As mentioned above, a decision to implement security measures is made before the ASU database is used. The analysis provided by the ASU is only one factor used by Judicial Security specialists in the OST and the districts to determine the level and potential duration of security. The ASU analysis itself does not direct whether security should be applied or what the security should be. These decisions are made by professionals based on their experience, training, and other factors such as the desires and circumstance surrounding the protectees.

In addition, the USMS recently reviewed cases with known outcomes for the period of 1997 through 2003. They were compared with the database of known outcomes that was last updated in 1996. The results showed the level of validity remains relatively high. The percentage results were (1996 data base listed first): specious 97.1/91; enhanced 6.4/5: and violent 2.2/4.

USMS Corrective Action:

A requirements analysis on updating the database is underway. It should be completed by March 15,2004. Once completed, the cost and time to complete the project will be determined.

RECOMMENDATION 3: Assign USMS representatives to all 56 FBI field office JTTF's and ensure effective liaison with intelligence agencies (e.g., the U.S. Secret Service National Threat Assessment Center, the Central Intelligence Agency, and the National Security Agency.

USMS Comments:

The USMS agrees that having a full time representative at all JTTF's is desirable. It should be noted that since September 11th, it has been able to increase the number of employees assigned to the task forces from less than ten (10) to forty-nine (49). This has been done without the

appropriation of positions specifically for this purpose. In addition, the draft report does not mention that the USMS:

- Chief of Intelligence Operations is a member of the FBI SIOC;
- Has assigned an employee of the Investigative Services Division to the CIA;
- Is working with the U.S. Capitol Police, Department of State Office of Diplomatic Security, and U.S. Secret Service National Threat Assessment Center to develop a Targeted Violence Information Sharing System.
- Has active and ongoing relationships with the NSA, NRO, NIMA, DOD Criminal Investigations Task Force, and the Law Enforcement Working Group of the Intelligence Community:

USMS Corrective Action:

The USMS will seek additional positions in the FY 2006 budget to station at least one full-time employee at each of the FBI JTTFs.

RECOMMENDATION 4: Create a centralized capability to identify, collect, analyze and share intelligence with USMS districts, as well as the USMS JTTF representatives and other intelligence liaisons.

USMS Comments:

The USMS agrees with this recommendation and prior to the review had already created an Office of Intelligence. A senior GS-15 Criminal Investigator with extensive experience in Judicial Security and as a U.S. Marshal and Chief Deputy U.S. Marshal has been designated as the Chief of this new office.

USMS Corrective Action:

The USMS will be seeking the resources needed to fully staff the Office of Intelligence as part of the FY 2006 budget process. In the meantime, the USMS will explore ways to provide additional staffing to the office on a temporary duty basis.

RECOMMENDATION 5: Require that all Chief Deputy U.S. Marshals and USMS JTTF representatives have Top Secret clearances and that each district has secure communications equipment.

USMS Comments:

While the USMS agrees with this recommendation, it is another example of where the draft report understates the efforts of the USMS. Prior to September 11th, only 889 employees held Secret or higher clearance. Currently 2,185 employees hold a Secret clearance or higher. This includes 94 U.S. Marshals and 77 Chief Deputies who hold a Top Secret Clearance. The remaining 14 Chief Deputies are being processed for Top Secret clearances (three Chief Deputy positions are vacant at this time). Of the 49 USMS employees assigned to JTTFs, 42 have Top Secret or Interim Top Secret Clearances. It is obvious by the progress made since September 11th that the USMS understands the importance of security clearances and is moving aggressively to ensure that all employees are appropriately cleared.

At the time the draft report was being compiled, it was well known that the USMS was committed to providing secure telephone communications equipment. Proof that this initiative was well underway is the fact that sixty three districts now have secure communication capability and that STE equipment for the remaining districts is on order. It is also important to point out that all USMS districts have had secure radio communication capability since that equipment first became available. Finally, the USMS has had an aggressive Operations Security (OpSec) program in place since 1997.

USMS Corrective Actions:

The remaining Chief Deputy Marshals and JTTF representatives will have Top Secret clearances within 30 days of completion of their OPM background investigations. Newly appointed Chief Deputy Marshals and JTTF representatives will have background investigations initiated within 15 days of appointment, and Interim Top Secret clearances within 30 days of appointment. The remaining STE units which were ordered from the NSA Contract are scheduled to arrive by the end of June 2004.

RECOMMENDATION 6: Revise the 1993 Judicial and Court Security Manual and the 1999 Offsite Security Booklet for Judicial Officers to establish risk- based standards and require after-action reports for high threat- trials and protective details.

USMS Comments:

While the USMS agrees with this recommendation, it is important to note that the basic information and guidance in both the Manual and the Booklet are still sound. There is nothing in either document that would jeopardize security if followed. In addition, the ongoing Judicial Security training that is provided to all law enforcement personnel during Basic, Advanced, Specialized and Supervisory/Management classes is regularly reviewed and updated as necessary. It should also be noted that this training is supplemented by ongoing meetings,

conferences, operational bulletins, and threat advisories which transmit the very latest intelligence and guidance on Judicial Security. Finally, while after action reports are important, major high threat trials and protective details are closely monitored or supervised by senior Criminal Investigators assigned to either the Judicial Security or Investigative Services Divisions. Therefore, lessons learned are not lost.

USMS Corrective Actions:

The USMS has recently completed a new protocol for conducting judicial threat assessments and has developed risk-based criteria to be used when planning high-risk trials, protective details, and threat investigations. They have been posted on the USMS intranet web site and copies are attached to this response. The Manual, Booklet, and after action-report requirements will be completed by the end of August 2004.

CONCLUSION:

In spite of its impressive record, the USMS is committed to the ongoing evaluation and improvement of the Judicial Security program. The USMS meets regularly with members of the Judicial Conference of the United States, the Administrative Office of U.S. Courts, the General Services Administration, and the U.S. Postal Service on matters of facility and judicial security. U.S. Marshals are required to meet regularly with their local judicial security committees and those judges assigned special security responsibilities. In addition to regular meetings, the Marshals are directed by USMS headquarters to convene special security meetings whenever threat information so justifies. Soon, each U.S. Marshal will be tasked to work with members of the local judicial family to develop individual Continuation of Operation Plans (COOP) as part of the government-wide Continuity of Government (COG) initiative. The USMS will continue to use all opportunities to enhance its Judicial Security capabilities.

APPENDIX III: THE OIG'S ANALYSIS OF THE USMS'S RESPONSE

On December 30, 2003, the Office of the Inspector General (OIG) sent copies of the draft report to the United States Marshals Service (USMS) with a request for written comments. The USMS responded to us in a memorandum dated February 4, 2004.

The USMS Response

The USMS's general concerns with our findings are its belief that we did not provide sufficient information about the USMS's efforts since September 11, 2001, to protect the Judiciary, and that some information presented in the report was inaccurate or incomplete. The USMS claims that the OIG failed "to demonstrate an even basic understanding of how the USMS Judicial Security process works" and misrepresents the effectiveness of the Judicial Security Program. Our disagreement with that statement is explained in the analysis that follows. Moreover, we note that although the USMS expressed concerns about some of the report's findings, it concurred with all six of the recommendations and agreed to implement them. Our detailed analysis of the USMS's response to our report and recommendations follows.

USMS's Efforts Since September 11, 2001

The USMS states that its highest priority is judicial security, and during the years before September 11, 2001, it "successfully secured thousands of high risk trials." The USMS states that after September 11, 2001, it "renewed and strengthened its commitment to protecting the Judiciary," and implemented numerous initiatives "to enhance an already strong Judicial Security program," which the USMS claims the OIG report does not acknowledge. The USMS provided four examples of its accomplishments, including the hiring of 807 new Deputy Marshals, the training of approximately 100 employees as threat investigators, the deployment of over 800 Automated External Defibrillators, and the purchase of new high capacity firearms for more than 4,000 Court Security Officers.

OIG Analysis. At the initiation of this review, we requested that the USMS provide a list of judicial security improvements since September 11, 2001, so that we could evaluate the improvements during our review. On June 13, 2003, the USMS provided a minimal list, consisting primarily of generic building security improvements implemented government-wide in the months subsequent to the September 11 terrorist attacks (Appendix A). No additional information of this nature was provided during our review until the February 4, 2004, USMS response to the draft report. Consequently, we did not have an opportunity to examine some of the post-September 11, 2001, efforts the USMS now cites, and we did not validate the accuracy of the new information or its relevance to improving the capability of the Judicial Security Program. However, the USMS's new claims about increased staff and equipment do not undermine the core criticisms our review made about the operation of the Judicial Security Program.

Inaccurate or Incomplete Information

The USMS also asserts that the report misrepresents the effectiveness of the USMS Judicial Security Program because it does not acknowledge the numerous trials that the USMS has successfully protected. The USMS states that "the draft report leaves an inaccurate, or at least, incomplete picture," and uses "anecdotal and/or incomplete information." The USMS cites four examples of information from the report that it considers to be inaccurate or incomplete.

1. The USMS believes that the OIG report incorrectly relied on two recent assaults on federal judges to question the effectiveness of its Judicial Security Program. The response states that "the USMS believes that one of the two incidents mentioned in the draft report was actually a random street robbery that had nothing to do with the judge's identity or duties."

OIG Analysis. The USMS's statement that one of the assaults we cited was a random street robbery is incorrect. The two assaults described in our report were cited in "The Attorney General's 2001 Performance Report, Strategic Goal Seven: Protect the Federal Judiciary." That report specifically describes assaults on two federal judges in their courtrooms.

2. The USMS believes that the OIG report incorrectly implies that Congress was concerned about the USMS's ability to secure the judiciary, when

Congress was actually only concerned about the USMS's failure to follow budgetary earmarks. The USMS challenges the OIG report citation of congressional concerns, stating that "[t]he draft report never fully explains what the [Congressional] concern actually was and whether or not it was validated." The USMS goes on to state that "Congress was concerned that the USMS was not using Judicial Security funding as it had been 'earmarked' in the appropriation." The USMS further states that the 2003 OIG audit "failed to find a single case where the USMS spent these funds other than as Congress intended."

OIG Analysis. The USMS suggestion that congressional concern was limited to a single issue (i.e., earmarks) is incorrect. The OIG report cites several concerns related to the effectiveness of the Judicial Security Program that Congress has expressed to the USMS in hearings, questions for the record, and other correspondence. These concerns include such issues as the criteria for establishing and removing protective details, protection of the judiciary during high-threat trials, and USMS participation on the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Forces (JTTFs). The report describes several of these concerns (see, for example, pages 2, 4, 16, 21, and 22), and recommends improvements to use the resources Congress has provided more effectively.

The USMS also mischaracterizes the finding of the 2003 OIG audit by stating that the audit "failed to find a single case where the USMS spent these funds other than as Congress intended." In fact, the audit found that because the USMS does not have a budget execution system that tracks changes, obligations, and expenditures to the budget estimates included in congressional spending instructions, the USMS could not demonstrate adherence to 7 of the 17 FY 2002 spending instructions from the Congress and 9 of the 22 FY 2003 spending instructions.[54]

3. The USMS states that it has no information that any judge is under an express death threat from a terrorist group. The USMS states that it "has no information that any judge is under such a threat," but it does state that

[54] Department of Justice, Office of the Inspector General, *Budget Execution in the United States Marshals Service During Fiscal Years 2002 and 2003*, Report No. 04-02, October 2003, pages 8 and 19.

"those judges who are at increased risk as a result of their participation in terrorist trials have the highest levels of security possible."

OIG Analysis. The discussion in the report regarding the personal protective measures that have been maintained on two judges for over eight years is based on our interviews with USMS headquarters and field personnel, as well as our review of documents which describe the threats that were the impetus for the protective measures. The specific statement that the two judges are under express death threats is our unclassified characterization of the description in intelligence documents regarding the threats. Although further discussion of the nature of the threats and how they were received is not appropriate for an unclassified document, we note that the long-term maintenance of these two protective details, supported by direct funding from Congress, would not be appropriate in the absence of a continuing identifiable threat.

4. The USMS objects to the report's conclusions regarding shortcomings in assessing threats, an ad hoc approach to security on high-threat trials and personal protective details, outdated policies, and ineffective allocation of resources. The USMS states that the report's "statements are made without a single example of when these alleged inadequacies resulted in a trial being disrupted or a member of the judicial family being injured."

OIG Analysis. The USMS's objections to our conclusions focus on the absence of realized threats or actual attacks, rather than on the increased risk to the federal judiciary that accrues from inadequate threat assessment, the lack of a centralized intelligence capability, and the lack of standards for protective measures. In so doing, the USMS response fails to fully comprehend the seriousness of those shortcomings. Our report shows that the process the USMS uses to analyze threats is outdated and untimely; the USMS itself recognized the lack of a centralized intelligence capability as a weakness; and that USMS standards for addressing high-threat trials are inadequate. We address each statement in the USMS response regarding specific shortcomings in turn:

- Shortcomings in assessing threats. As documented in our report, the USMS does not meet its own standards for assessing threats against the judiciary. Further, internal studies have recognized that the

USMS does not have a program for collecting and assessing intelligence and using that intelligence to analyze threats.

- Ad hoc approach to security on high-threat trials and personal protective details. The USMS defends its ad hoc approach to high-threat trial security by stating that "requirements for every high threat trial…are determined on a case-by-case basis…" and asserting that its operational plans are implemented by "personnel who have received specialized training and who utilize the latest in high tech security equipment." Our conclusion that uniform judicial security standards are needed is based in part on discussions with USMS staff in several districts. The U.S. Marshals and Deputy Marshals we interviewed emphasized the importance of consistent security measures and complained of insufficient criteria for determining the appropriateness of existing measures to guide districts in selecting protections when developing operational plans. We did not assess whether specific protective techniques described in operational plans were "adequate" or "appropriate." Our report concludes that without effective current standards, and routine after-action reports, the USMS cannot identify inconsistent protections, needed improvements, or successful protective measures for ensuring the security of the federal judiciary.

- Outdated policies. Our conclusions about the lack of up-to-date policies were based on the concerns expressed to us by personnel in the USMS districts who must determine and implement protection techniques that are "adequate" or "appropriate." Our report states:

  > [T]en U.S. Marshals and Deputy Marshals that we interviewed noted that the guidance in the Manual does not address many types of trials that present significant risks to the judiciary, such as criminal cases involving espionage, prosecutions of gang violence, and cases with cooperating witnesses. Moreover, a significant defining issue in recent high-threat trials – that the defendants are associated with international terrorist groups – is not included.

- Ineffectively deployed equipment. Our conclusions regarding the deployment of equipment were based on our discussions with field

personnel regarding the availability and use of "high tech" security equipment. For example, we found that one district did not use its new explosives detector because of a lack guidance from headquarters:

> [A] district we visited did not use its new "Itemiser[3] Trace Explosive Detector" during a high-threat trial because the district was waiting for guidance from USMS headquarters on where to deploy the equipment (public or freight entrance), who should be screened, and what protective measures should be taken if suspected explosives are detected (e.g., retest for false positive or immediately evacuate the building).

- Ineffective allocation of resources among threats. We could not validate the USMS's comment that "94 per cent of all requests for special assignment resources are approved." In fact, during our review, in response to our request for funding data on high-threat trials, a representative of the Judicial Security Division (JSD) told us that, "JSD does not keep a data bank for the amount of requests that come to JSD, JSD keeps a data bank on the amount of requests that are approved." Moreover, "approval" does not mean that *all* resources requested were provided.

Effectiveness of the Judicial Security Program

The USMS response states as a general theme that the OIG report misrepresents the effectiveness of the Judicial Security Program. To the contrary, our report appropriately warns of significant vulnerabilities in critical elements of the USMS's program. The intelligence and threat assessment capabilities we examined were implemented in response to the assassinations of two federal judges in 1988 and 1989. The fact that no member of the judiciary has been assassinated in the past 15 years is not a valid response to the need to correct shortcomings we identified in the USMS's threat analysis capability or the lack of a centralized intelligence capability. Further, the USMS's argument that neither of the judges attacked in 1988 and 1989 was overtly threatened prior to being attacked reinforces our concern that the USMS lacks the intelligence and analytical capabilities it needs to effectively and timely detect and respond to nascent threats.

Finally, the USMS's argument that the lack of recent attacks equates to a lack of vulnerabilities reinforces our conclusion that the USMS needs to improve its ability to self-assess its operations and recognize weaknesses before failures occur. To meets its Strategic Performance Measure of allowing "zero assaults" on the judiciary, we believe the USMS should improve its ability to recognize and take prompt action on deficiencies, such as the ones we identified.

RECOMMENDATIONS

Recommendation 1: Ensure that all threats to the judiciary are assessed within established timeframes.

Summary of USMS Response. The USMS agrees with the recommendation that all threats should be assessed according to policy. The USMS will revise its policy on timeframes for the Analytical Support Unit (ASU) to complete assessments. The new policy will establish criteria that categorize requests according to urgency. Once the policy is implemented, adherence to the timeframes will be made a factor in the annual performance evaluations of the ASU staff. The USMS estimates that the new policy will be implemented by the end of August 2004. The USMS also will review the workload of the ASU and will request additional resources during the FY 2006 budget process, if necessary.

OIG Analysis. Recommendation 1 is Resolved – Open. The actions planned by the USMS to revise its policy concerning ASU assessment timeframes are responsive to our recommendation. Please provide us with a copy of the new policy by September 30, 2004.

Recommendation 2: Update the historical threat database or develop a new database to perform comparative assessments.

Summary of USMS Response. The USMS agrees with the recommendation that the threat database should be updated. In addition, the USMS believes that the threat database is a valuable part of the overall threat assessment and response process. However, the USMS believes that the draft report greatly overstates the role of the database and the adverse impact of not

having it current. The USMS bases its assessment, at least in part, on a recent validation of the historical threat database prompted by our draft report, concluding that the validity of the database remains relatively high. This may be true for resource allocations based on the database, but an estimate of validity based on results alone has little or no applicability to the use of the database as an assessment tool. Similar results may be attributable to different variables, particularly when the database has not been updated since 1996. The USMS stated that a requirements analysis on updating the database is underway and should be completed by March 15, 2004. Once completed, the cost and time to complete the project will be determined.

OIG Analysis. Recommendation 2 is Resolved – Open. We disagree with the USMS's opinion that the report overstates the role of the historical threat database and the adverse impact of it being out-of-date. The database was part of the improvements implemented after two judges were assassinated in the 1980s, and it is intended to, among other things, assist in ensuring that appropriate personal protective measures are taken at the district level. An out-of-date threat assessment tool affects it value and decreases the potential that a threat against a member of the federal judiciary will be assessed accurately. Notwithstanding the USMS's assertions regarding the database, the actions planned by the USMS are responsive to our recommendation. Please provide us with a copy of the completed requirements analysis and the project's implementation plan by April 30, 2004.

Recommendation 3: Assign full-time representatives to all 56 FBI field office JTTFs and ensure effective USMS liaison with intelligence agencies (e.g., the U.S. Secret Service's National Threat Assessment Center, the Central Intelligence Agency, and the National Security Agency).

Summary of USMS Response. The USMS agrees that having a full-time representative on all JTTFs is desirable. The USMS states that it has been steadily increasing its JTTF representation since September 11, 2001, without the appropriation of positions specifically for that purpose. The USMS will seek additional positions in the FY 2006 budget to assign at least one full-time employee on each of the FBI's JTTFs. In addition, the USMS stated that it has assigned personnel to, and has an active and ongoing relationship with, external intelligence agencies.

OIG Analysis. Recommendation 3 is Resolved – Open. The actions undertaken and planned by the USMS are generally responsive to our

recommendation. However, the delay until a request for additional resources is submitted and approved postpones addressing the USMS's intelligence vulnerability until 2006 or later. By April 30, 2004, and quarterly thereafter until full representation on JTTFs is achieved, we request that the USMS provide us with a roster of all its full-time and part-time representatives on JTTFs.

Recommendation 4: Create a centralized capability to identify, collect, analyze, and share intelligence with USMS districts, as well as with the USMS JTTF representatives and other intelligence liaisons.

Summary of USMS Response. The USMS agrees with the recommendation. The USMS response states that prior to the OIG review it already had created an Office of Intelligence with a senior Criminal Investigator designated as its Chief. To establish the office as a functioning entity, the USMS will seek the resources needed to fully staff the office as part of the FY 2006 budget process. In the meantime, the USMS will explore ways to provide additional staffing to the office on a temporary duty basis.

OIG Analysis. Recommendation 4 is Resolved – Open. The actions undertaken and planned by the USMS are responsive to our recommendation. Please provide us with a copy of the Office of Intelligence's mission statement, staffing requirements, and implementation plan by April 30, 2004.

Recommendation 5: Require that all Chief Deputy Marshals and USMS JTTF representatives have Top Secret clearances, and ensure that each district has secure communication equipment.

Summary of USMS Response. The USMS agrees with the recommendation. However, the USMS states that the OIG did not address the progress that the USMS has made in increasing the number of employees with security clearances since September 11, 2001. According to the USMS, all 94 U.S. Marshals and 77 of the 94 Chief Deputy Marshals currently hold a Top Secret clearance. The remaining 14 Chief Deputies are being processed for Top Secret clearances (three Chief Deputy positions are vacant at this time). The USMS also responded that of the 49 USMS employees it has assigned to JTTFs, 42 have Top Secret or interim Top Secret clearances.

The USMS responded that the current Chief Deputy Marshals and JTTF representatives without Top Secret clearances will receive their clearances within 30 days of completion of their OPM background investigations. In addition, newly appointed Chief Deputy Marshals and JTTF representatives will have background investigations initiated within 15 days of their appointment, and interim Top Secret clearances within 30 days of appointment.

Concerning the issue of secure telephone communications equipment, the USMS states that it has increased the number of districts with this capability to 63 (from 51 on August 20, 2003) and that this equipment is on order for the other 31 districts. The remaining secure telephone communications equipment is scheduled to be deployed by June 30, 2004.

OIG Analysis. Recommendation 5 is Resolved – Open. The actions undertaken and planned by the USMS are responsive to our recommendation. Please provide us with a copy of the USMS policy for issuance of security clearances by April 30, 2004. Also, please include the clearance information for each representative on the quarterly reports requested under recommendation 3. In addition, please provide us with a status report on the installation of secure telephone communications equipment in each of the 94 districts by July 30, 2004.

Recommendation 6: Revise the 1993 *Judicial and Court Security Manual* and the 1999 *Offsite Security Booklet for Judicial Officers* to establish risk-based standards and require after-action reports for high-threat trials and protective details.

Summary of USMS Response. The USMS agrees with the recommendation. However, the USMS states that the basic information and guidance in both the 1993 *Judicial and Court Security Manual* and the 1999 *Offsite Security Booklet for Judicial Officers* are still sound and that nothing in either document would jeopardize security if followed.

The USMS recently completed a new protocol for conducting judicial threat assessments and has developed risk-based criteria to be used when planning high-risk trials, protective details, and threat investigations. The USMS has posted this protocol and risk-based criteria on the USMS intranet web site and provided copies to the OIG. Further, the USMS states that revisions to the 1993 *Judicial and Court Security Manual*, the 1999 *Offsite*

Security Booklet for Judicial Officers, and after action-report requirements will be completed by the end of August 2004.

OIG Analysis. Recommendation 6 is Resolved – Open. The actions undertaken and planned by the USMS are responsive to our recommendation. The USMS's statement that following the guidance in the 1993 and 1999 documents would not in itself jeopardize security is not persuasive. The documents are out-of-date and the guidance contained in them is incomplete. The revisions that the USMS agrees to make must include all the actions necessary to ensure the protection of the federal judiciary. Please provide us with a copy of the revised *Judicial and Court Security Manual, the Offsite Security Booklet for Judicial Officers*, and after action-reporting requirements by September 30, 2004.